Configuring RMON and RMON2

BayRS Version 13.00
Site Manager Software Version 7.00

BCC Version 5.04

Part No. 303539-A Rev 00
October 1998

Bay Networks Where Information Flows.™

4401 Great America Parkway
Santa Clara, CA 95054

8 Federal Street
Billerica, MA 01821

Copyright © 1998 Bay Networks, Inc.

All rights reserved. Printed in the USA. October 1998.

The information in this document is subject to change without notice. The statements, configurations, technical data, and recommendations in this document are believed to be accurate and reliable, but are presented without express or implied warranty. Users must take full responsibility for their applications of any products specified in this document. The information in this document is proprietary to Bay Networks, Inc.

The software described in this document is furnished under a license agreement and may only be used in accordance with the terms of that license. A summary of the Software License is included in this document.

Trademarks

ACE, AFN, AN, BCN, BLN, BN, BNX, CN, FRE, LN, Optivity, PPX, Quick2Config, and Bay Networks are registered trademarks and Advanced Remote Node, ANH, ARN, ASN, BayRS, BaySecure, BayStack, BayStream, BCC, BCNX, BLNX, EZ Install, EZ Internetwork, EZ LAN, FN, IP AutoLearn, PathMan, RouterMan, SN, SPEX, Switch Node, System 5000, and the Bay Networks logo are trademarks of Bay Networks, Inc.

Microsoft, MS, MS-DOS, Win32, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

All other trademarks and registered trademarks are the property of their respective owners.

Restricted Rights Legend

Use, duplication, or disclosure by the United States Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Notwithstanding any other license agreement that may pertain to, or accompany the delivery of, this computer software, the rights of the United States Government regarding its use, reproduction, and disclosure are as set forth in the Commercial Computer Software-Restricted Rights clause at FAR 52.227-19.

Statement of Conditions

In the interest of improving internal design, operational function, and/or reliability, Bay Networks, Inc. reserves the right to make changes to the products described in this document without notice.

Bay Networks, Inc. does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Portions of the code in this software product may be Copyright © 1988, Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms of such portions are permitted, provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that such portions of the software were developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from such portions of the software without specific prior written permission.

SUCH PORTIONS OF THE SOFTWARE ARE PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In addition, the program and information contained herein are licensed only pursuant to a license agreement that contains restrictions on use and disclosure (that may incorporate by reference certain limitations and notices imposed by third parties).

Bay Networks, Inc. Software License Agreement

NOTICE: Please carefully read this license agreement before copying or using the accompanying software or installing the hardware unit with pre-enabled software (each of which is referred to as "Software" in this Agreement). BY COPYING OR USING THE SOFTWARE, YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT. THE TERMS EXPRESSED IN THIS AGREEMENT ARE THE ONLY TERMS UNDER WHICH BAY NETWORKS WILL PERMIT YOU TO USE THE SOFTWARE. If you do not accept these terms and conditions, return the product, unused and in the original shipping container, within 30 days of purchase to obtain a credit for the full purchase price.

1. License Grant. Bay Networks, Inc. ("Bay Networks") grants the end user of the Software ("Licensee") a personal, nonexclusive, nontransferable license: a) to use the Software either on a single computer or, if applicable, on a single authorized device identified by host ID, for which it was originally acquired; b) to copy the Software solely for backup purposes in support of authorized use of the Software; and c) to use and copy the associated user manual solely in support of authorized use of the Software by Licensee. This license applies to the Software only and does not extend to Bay Networks Agent software or other Bay Networks software products. Bay Networks Agent software or other Bay Networks software products are licensed for use under the terms of the applicable Bay Networks, Inc. Software License Agreement that accompanies such software and upon payment by the end user of the applicable license fees for such software.

2. Restrictions on use; reservation of rights. The Software and user manuals are protected under copyright laws. Bay Networks and/or its licensors retain all title and ownership in both the Software and user manuals, including any revisions made by Bay Networks or its licensors. The copyright notice must be reproduced and included with any copy of any portion of the Software or user manuals. Licensee may not modify, translate, decompile, disassemble, use for any competitive analysis, reverse engineer, distribute, or create derivative works from the Software or user manuals or any copy, in whole or in part. Except as expressly provided in this Agreement, Licensee may not copy or transfer the Software or user manuals, in whole or in part. The Software and user manuals embody Bay Networks' and its licensors' confidential and proprietary intellectual property. Licensee shall not sublicense, assign, or otherwise disclose to any third party the Software, or any information about the operation, design, performance, or implementation of the Software and user manuals that is confidential to Bay Networks and its licensors; however, Licensee may grant permission to its consultants, subcontractors, and agents to use the Software at Licensee's facility, provided they have agreed to use the Software only in accordance with the terms of this license.

3. Limited warranty. Bay Networks warrants each item of Software, as delivered by Bay Networks and properly installed and operated on Bay Networks hardware or other equipment it is originally licensed for, to function substantially as described in its accompanying user manual during its warranty period, which begins on the date Software is first shipped to Licensee. If any item of Software fails to so function during its warranty period, as the sole remedy Bay Networks will at its discretion provide a suitable fix, patch, or workaround for the problem that may be included in a future Software release. Bay Networks further warrants to Licensee that the media on which the Software is provided will be free from defects in materials and workmanship under normal use for a period of 90 days from the date Software is first shipped to Licensee. Bay Networks will replace defective media at no charge if it is returned to Bay Networks during the warranty period along with proof of the date of shipment. This warranty does not apply if the media has been damaged as a result of accident, misuse, or abuse. The Licensee assumes all responsibility for selection of the Software to achieve Licensee's intended results and for the installation, use, and results obtained from the Software. Bay Networks does not warrant a) that the functions contained in the software will meet the Licensee's requirements, b) that the Software will operate in the hardware or software combinations that the Licensee may select, c) that the operation of the Software will be uninterrupted or error free, or d) that all defects in the operation of the Software will be corrected. Bay Networks is not obligated to remedy any Software defect that cannot be reproduced with the latest Software release. These warranties do not apply to the Software if it has been (i) altered, except by Bay Networks or in accordance with its instructions; (ii) used in conjunction with another vendor's product, resulting in the defect; or (iii) damaged by improper environment, abuse, misuse, accident, or negligence. THE FOREGOING WARRANTIES AND LIMITATIONS ARE EXCLUSIVE REMEDIES AND ARE IN LIEU OF ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Licensee is responsible for the security of

its own data and information and for maintaining adequate procedures apart from the Software to reconstruct lost or altered files, data, or programs.

4. Limitation of liability. IN NO EVENT WILL BAY NETWORKS OR ITS LICENSORS BE LIABLE FOR ANY COST OF SUBSTITUTE PROCUREMENT; SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES; OR ANY DAMAGES RESULTING FROM INACCURATE OR LOST DATA OR LOSS OF USE OR PROFITS ARISING OUT OF OR IN CONNECTION WITH THE PERFORMANCE OF THE SOFTWARE, EVEN IF BAY NETWORKS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT SHALL THE LIABILITY OF BAY NETWORKS RELATING TO THE SOFTWARE OR THIS AGREEMENT EXCEED THE PRICE PAID TO BAY NETWORKS FOR THE SOFTWARE LICENSE.

5. Government Licensees. This provision applies to all Software and documentation acquired directly or indirectly by or on behalf of the United States Government. The Software and documentation are commercial products, licensed on the open market at market prices, and were developed entirely at private expense and without the use of any U.S. Government funds. The license to the U.S. Government is granted only with restricted rights, and use, duplication, or disclosure by the U.S. Government is subject to the restrictions set forth in subparagraph (c)(1) of the Commercial Computer Software—Restricted Rights clause of FAR 52.227-19 and the limitations set out in this license for civilian agencies, and subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause of DFARS 252.227-7013, for agencies of the Department of Defense or their successors, whichever is applicable.

6. Use of Software in the European Community. This provision applies to all Software acquired for use within the European Community. If Licensee uses the Software within a country in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May, 1991, will apply to the examination of the Software to facilitate interoperability. Licensee agrees to notify Bay Networks of any such intended examination of the Software and may procure support and assistance from Bay Networks.

7. Term and termination. This license is effective until terminated; however, all of the restrictions with respect to Bay Networks' copyright in the Software and user manuals will cease being effective at the date of expiration of the Bay Networks copyright; those restrictions relating to use and disclosure of Bay Networks' confidential information shall continue in effect. Licensee may terminate this license at any time. The license will automatically terminate if Licensee fails to comply with any of the terms and conditions of the license. Upon termination for any reason, Licensee will immediately destroy or return to Bay Networks the Software, user manuals, and all copies. Bay Networks is not liable to Licensee for damages in any form solely by reason of the termination of this license.

8. Export and Re-export. Licensee agrees not to export, directly or indirectly, the Software or related technical data or information without first obtaining any required export licenses or other governmental approvals. Without limiting the foregoing, Licensee, on behalf of itself and its subsidiaries and affiliates, agrees that it will not, without first obtaining all export licenses and approvals required by the U.S. Government: (i) export, re-export, transfer, or divert any such Software or technical data, or any direct product thereof, to any country to which such exports or re-exports are restricted or embargoed under United States export control laws and regulations, or to any national or resident of such restricted or embargoed countries; or (ii) provide the Software or related technical data or information to any military end user or for any military end use, including the design, development, or production of any chemical, nuclear, or biological weapons.

9. General. If any provision of this Agreement is held to be invalid or unenforceable by a court of competent jurisdiction, the remainder of the provisions of this Agreement shall remain in full force and effect. This Agreement will be governed by the laws of the state of California.

Should you have any questions concerning this Agreement, contact Bay Networks, Inc., 4401 Great America Parkway, P.O. Box 58185, Santa Clara, California 95054-8185.

LICENSEE ACKNOWLEDGES THAT LICENSEE HAS READ THIS AGREEMENT, UNDERSTANDS IT, AND AGREES TO BE BOUND BY ITS TERMS AND CONDITIONS. LICENSEE FURTHER AGREES THAT THIS AGREEMENT IS THE ENTIRE AND EXCLUSIVE AGREEMENT BETWEEN BAY NETWORKS AND LICENSEE, WHICH SUPERSEDES ALL PRIOR ORAL AND WRITTEN AGREEMENTS AND COMMUNICATIONS BETWEEN THE PARTIES PERTAINING TO THE SUBJECT MATTER OF THIS AGREEMENT. NO DIFFERENT OR ADDITIONAL TERMS WILL BE ENFORCEABLE AGAINST BAY NETWORKS UNLESS BAY NETWORKS GIVES ITS EXPRESS WRITTEN CONSENT, INCLUDING AN EXPRESS WAIVER OF THE TERMS OF THIS AGREEMENT.

Contents

Preface

Before You Begin xiii
Text Conventions xiv
Acronyms xv
Bay Networks Technical Publications xvi
How to Get Help xvi

Chapter 1
RMON and RMON2 Overview

RMON MIB 1-1
RMON2 MIB 1-3
RMON and RMON2 Support on Bay Networks Routers 1-8
RMON and RMON2 Architecture 1-9
Data Collection Module (DCM) 1-11
DCM Agent Software 1-11
DCM Middleware (DCMMW) 1-11
RMON Agent Software 1-11
RMON Network Management Software 1-12
Optivity Analysis for UNIX 1-12
Optivity LAN 1-15
Optivity Analysis for Windows NT 1-16

Chapter 2
Starting RMON and RMON2 on AN/ANH and ARN Routers

Router Hardware and Software Prerequisites 2-2
Starting Configuration Tools 2-4

Starting RMON and RMON2 2-4
Preparing a Configuration File 2-4
Configuring an Ethernet DCM for AN/ANH Routers 2-5
Configuring an Ethernet DCM for ARN Routers 2-7
Customizing the Ethernet DCM 2-9

Chapter 3
Configuring Mini-RMON on an ARN 100 Router

Configuration Considerations 3-2
Starting Mini-RMON 3-2
Preparing a Configuration File 3-3
Enabling Mini-RMON Data Collection 3-3
Disabling Mini-RMON Data Collection 3-5

Chapter 4
Customizing a DCM for RMON and RMON2

Disabling the Ethernet DCM 4-2
Specifying RMON or RMON2 Data Collection 4-3
Specifying the Configuration Mode 4-6
Saving the Configuration Information 4-7
Configuring the DCM Image on the Router 4-9
Modifying Default RMON MIB Group Parameters 4-12
Specifying the Maximum Number of RMON Hosts 4-12
Enabling and Disabling the RMON Host Control Table 4-14
Enabling and Disabling the RMON Matrix Control Table 4-16
Rebooting the Ethernet DCM 4-18
Deleting the Ethernet DCM Software Subsystem 4-19
Using the Technician Interface to Manage a DCM 4-20

Appendix A
Monitoring the DCM Using the BCC show Command

show rmon dcm A-2

Appendix B
Ethernet DCM Parameters

Appendix C
RMON and RMON2 MIB Groups

RMON MIB Groups C-1
RMON MIB Group Controls and Functions C-2
Statistics Group C-2
History Group C-2
Host Group C-3
HostTopN Group C-3
Matrix Group C-3
Filter Group C-3
Capture Group C-4
Alarm Group C-4
Event Group C-5
Event Trap Considerations C-6
RMON2 MIB Groups C-6
Protocol Directory Group C-7
Protocol Distribution Group C-8
Address Mapping Group C-9
Network Layer Host Group C-9
Application Layer Host Group C-9
Network Layer Matrix Group C-9
Application Layer Matrix Group C-10
Memory Requirements for RMON Groups C-11
Statistics Group C-12
History Group C-12
Host Group C-13
HostTopN Group C-14
Matrix Group C-14
Filter and Capture Groups C-15
Alarm and Event Groups C-16

Appendix D
Upgrading the DCM Software Image

Verifying Minimum DCM Requirements D-1
Upgrading the DCM Software Image D-2
Using Site Manager D-3
Using the Technician Interface D-5
Sample Display: dcmload.bat D-7

Index

Figures

Figure 1-1. RMON and RMON2 in the OSI Model 1-4
Figure 1-2. RMON/RMON2 MIB Tree 1-7
Figure 1-3. RMON/RMON2 Architecture 1-10
Figure C-1. Protocol Directory Statistics C-7
Figure C-2. Protocol Distribution Statistics C-8
Figure C-3. Application Layer Matrix Statistics C-10
Figure D-1. Choosing DCMMW Global Configuration Parameters D-3
Figure D-2. Edit Base Module DCM Parameters Window D-4

Tables

Table 1-1. RMON MIB Groups 1-2
Table 1-2. RMON2 MIB Groups 1-5
Table 1-3. Summary of RMON and RMON2 Support 1-8
Table 1-4. Optivity Analysis for UNIX RMON-Based Tools 1-13
Table 2-1. AN/ANH Requirements for Using RMON and RMON2 2-2
Table 2-2. ARN Requirements for Using RMON and RMON2 2-3
Table C-1. DRAM and RMON Memory Size C-11
Table C-2. Maximum Number of Hosts C-13
Table C-3. Default Size for Capture Buffer C-15

Preface

This guide describes configuring and managing an Ethernet remote monitoring (RMON) data collection module (DCM) in a Bay Networks® BayStack™ router. The BayStack family of routers includes the following platforms:

- Access Node (AN®)
- Access Node Hub (ANH™)
- Advanced Remote Node™ (ARN™)

You can use the Bay Command Console (BCC™) or Site Manager to configure RMON and RMON2 on a router. In this guide, you will find instructions for using both the BCC and Site Manager.

Before You Begin

Before using this guide, you must complete the following procedures. For a new router:

- Install the router (refer to the installation guide that came with your router).
- Connect the router to the network and create a pilot configuration file (refer to *Quick-Starting Routers* or *Configuring BayStack Remote Access).*

Make sure that you are running the latest version of Bay Networks BayRS™ and Site Manager software. For information about upgrading BayRS and Site Manager, see the upgrading guide for your version of BayRS.

Text Conventions

This guide uses the following text conventions:

angle brackets (< >)	Indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when entering the command. Example: If the command syntax is: **ping** *<ip_address>*, you enter: **ping 192.32.10.12**
bold text	Indicates text that you need to enter and command names and options. Example: Enter **show ip** {**alerts** | **routes**} Example: Use the **dinfo** command.
italic text	Indicates file and directory names, new terms, book titles, and variables in command syntax descriptions. Where a variable is two or more words, the words are connected by an underscore. Example: If the command syntax is: **show at** *<valid_route>* *valid_route* is one variable and you substitute one value for it.
`screen text`	Indicates system output, for example, prompts and system messages. Example: `Set Bay Networks Trap Monitor Filters`
separator (>)	Shows menu paths. Example: Protocols > IP identifies the IP option on the Protocols menu.
vertical line (|)	Separates choices for command keywords and arguments. Enter only one of the choices. Do not type the vertical line when entering the command. Example: If the command syntax is: **show ip** {**alerts** | **routes**}, you enter either: **show ip alerts** or **show ip routes**, but not both.

Acronyms

ASN.1	abstract syntax notation
CMIP	Common Management Information Protocol
DCM	data collection module
DCMMW	data collection module middleware
DLCI	data link control interface
DRAM	dynamic random access memory
FDDI	Fiber Distributed Data Interface
IP	Internet Protocol
LRU	least recently used
MAC	media access control
MIB	management information base
NVRAM	nonvolatile random access memory
PDU	protocol data unit
PVC	permanent virtual circuit
RFC	Request for Comments
RIP	Routing Information Protocol
RMON	remote monitoring
SNMP	Simple Network Management Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
WAN	wide area network

Bay Networks Technical Publications

You can now print Bay Networks technical manuals and release notes free, directly from the Internet. Go to *support.baynetworks.com/library/tpubs/*. Find the Bay Networks product for which you need documentation. Then locate the specific category and model or version for your hardware or software product. Using Adobe Acrobat Reader, you can open the manuals and release notes, search for the sections you need, and print them on most standard printers. You can download Acrobat Reader free from the Adobe Systems Web site, *www.adobe.com*.

You can purchase Bay Networks documentation sets, CDs, and selected technical publications through the Bay Networks Collateral Catalog. The catalog is located on the World Wide Web at *support.baynetworks.com/catalog.html* and is divided into sections arranged alphabetically:

- The “CD ROMs” section lists available CDs.
- The “Guides/Books” section lists books on technical topics.
- The “Technical Manuals” section lists available printed documentation sets.

Make a note of the part numbers and prices of the items that you want to order. Use the “Marketing Collateral Catalog description” link to place an order and to print the order form.

How to Get Help

For product assistance, support contracts, or information about educational services, go to the following URL:

http://www.baynetworks.com/corporate/contacts/

Or telephone the Bay Networks Technical Solutions Center at:

800-2LANWAN

Chapter 1
RMON and RMON2 Overview

RMON and RMON2 are MIB standards developed to provide powerful remote troubleshooting and monitoring within a LAN segment and across an enterprise network. This chapter includes the following information:

Topic	Page
RMON MIB	1-1
RMON2 MIB	1-3
RMON and RMON2 Support on Bay Networks Routers	1-8
RMON and RMON2 Architecture	1-9

RMON MIB

RMON is a standard MIB that defines current and historical statistics and control objects at the media access control (MAC) layer, allowing you to capture real-time information across the entire network. The RMON standard is an SNMP MIB definition described in RFC 1757 (formerly 1271) for Ethernet.

The RMON MIB provides a standard method for monitoring the basic operations of the Ethernet network, providing interoperability between Simple Network Management (SNMP) management stations and monitoring agents. RMON also provides a powerful alarm and event mechanism for setting thresholds and for notifying you of changes in network behavior.

You can use RMON to analyze and monitor network traffic data within remote LAN segments from a central location, enabling you to detect, isolate, diagnose, and report potential and actual network problems before they escalate to crisis situations. For example, the Ethernet DCM can identify the hosts on a network that generate the most traffic or errors.

RMON allows you to set up automatic histories, which the RMON agent collects over a period of time, providing trending data on such basic statistics as utilization, collisions, and so forth. Using a network management application such as Optivity LAN™ or Optivity Analysis™, you can retrieve histories to understand network usage patterns. Because RMON automates this data collection and provides better data to the planning process, the process is easier and the outcome more accurate.

Bay Networks implements seven RMON MIB groups in its RMON agent, and the alarm and event groups in its base module for BayStack AN/ANH and ARN routers. Table 1-1 summarizes the RMON MIB groups. For detailed information about the RMON MIB groups, see Appendix C, "RMON and RMON2 MIB Groups."

Table 1-1. RMON MIB Groups

Group	Lets You
Statistics	Analyze the operational effectiveness of your network. Statistics include packets, octets, broadcasts, multicasts, dropped packets, soft errors, and packet size distribution.
History	Analyze traffic trends based on historical data.
Host	Collect information for each host on the segment.
HostTopN	Reduce network overhead by looking at the most active nodes.
Matrix	Report on traffic and errors between any host pair.
Filter	Define criteria for capturing specific information.
Capture	Copy packets for analysis.
Alarm	Report on changes in network characteristics based on thresholds for any MIB variable of interest.
Event	Log events based on thresholds that you define. You can use these statistics to initiate functions such as data capture or instance counts to isolate specific portions of your network.

RMON2 MIB

RMON2 is a standard MIB that extends the scope of the RMON MIB beyond the MAC layer to provide statistics on network and application layer traffic (layers 3 through 7 of the OSI model). By monitoring higher-layer protocols, you can get an internetwork or enterprise-wide view of network traffic, enabling you to:

- Identify which systems are communicating with which servers and what applications they are using.
- Identify which devices are sending and receiving which types of traffic.

Using this knowledge of traffic patterns, you can strategically place users and resources in the correct location on the network to optimize performance and reduce costs.

Figure 1-1 shows the level of visibility that RMON and RMON2 provide within a LAN segment and within a network at each layer of the OSI model.

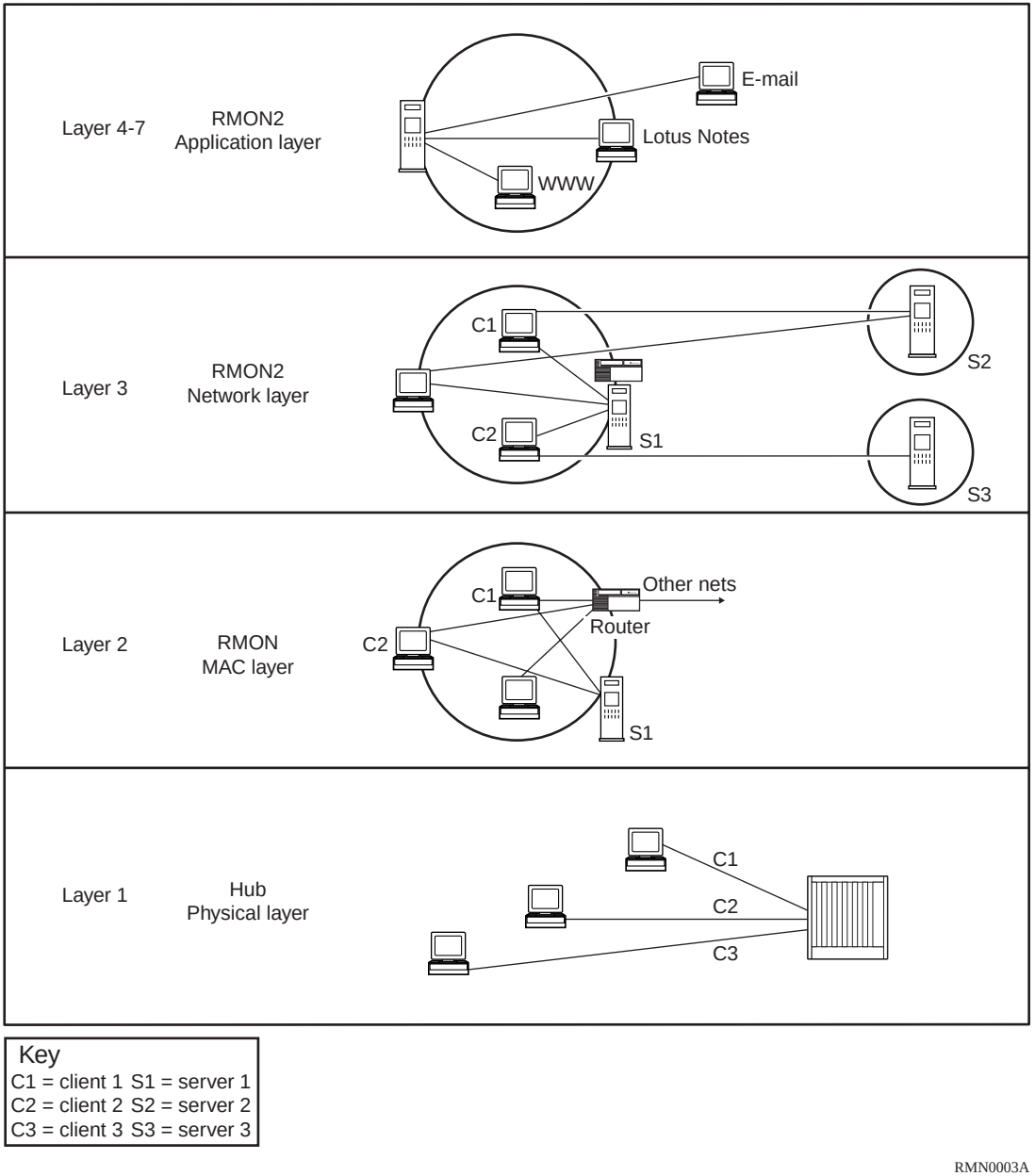

Figure 1-1. RMON and RMON2 in the OSI Model

With RMON2, you can also troubleshoot network problems faster and more accurately using statistics from the network layer matrix table, which shows the protocol-specific traffic between communicating pairs of systems.

For example, with RMON, you can learn that a particular server is inactive because it fails to transmit packets. With RMON2, you can diagnose the more difficult problem that occurs when the system is active but a particular protocol stack is malfunctioning.

RMON2 provides address translation capabilities that bind MAC-layer addresses to network-layer addresses, making all addresses easier to read and remember. You can detect duplicate addresses, which helps to solve a common problem that disrupts network routers and virtual LANs.

RMON2 allows you to collect the historical data of any counter in the system, rather than only a predefined set of statistics. For example, you can collect historical data on a specific file server or a specific router-to-router connection.

RMON2 also lets you configure more flexible and efficient filters to support higher-layer protocols.

Bay Networks implements seven RMON2 MIB groups in its RMON2 agent for BayStack AN/ANH and ARN routers. Table 1-2 summarizes the RMON2 MIB groups. For more detailed information about the RMON2 MIB groups, see Appendix C, "RMON and RMON2 MIB Groups."

Table 1-2. RMON2 MIB Groups

Group	Lets You
Protocol Directory	Compile a master directory of all protocols that the Ethernet DCM can interpret.
Protocol Distribution	Aggregate statistics on the amount of traffic generated by each protocol, per LAN segment, or for each layer in the protocol stack.
Address Mapping	Connect port numbers, MAC addresses, and network addresses.
Network Layer Host	Obtain statistics on the traffic of specific hosts (in/out, packets, octets, and so forth) based on the network layer address.

(continued)

Table 1-2. RMON2 MIB Groups *(continued)*

Group	Lets You
Application Layer Host	Obtain statistics on the traffic of specific hosts (in/out, packets, octets, and so forth) based on the network layer address.
Network Layer Matrix	Obtain statistics on the traffic between pairs of hosts (in/out, packets, octets, and so forth) based on the network layer address.
Application Layer Matrix	Obtain statistics on the traffic between pairs of hosts (in/out, packets, octets, and so forth) based on the application layer address.

For more information about RMON2 MIB groups, see Appendix C, "RMON and RMON2 MIB Groups."

Figure 1-2 illustrates the RMON/RMON2 MIB tree, showing RMON and RMON2 MIB groups.

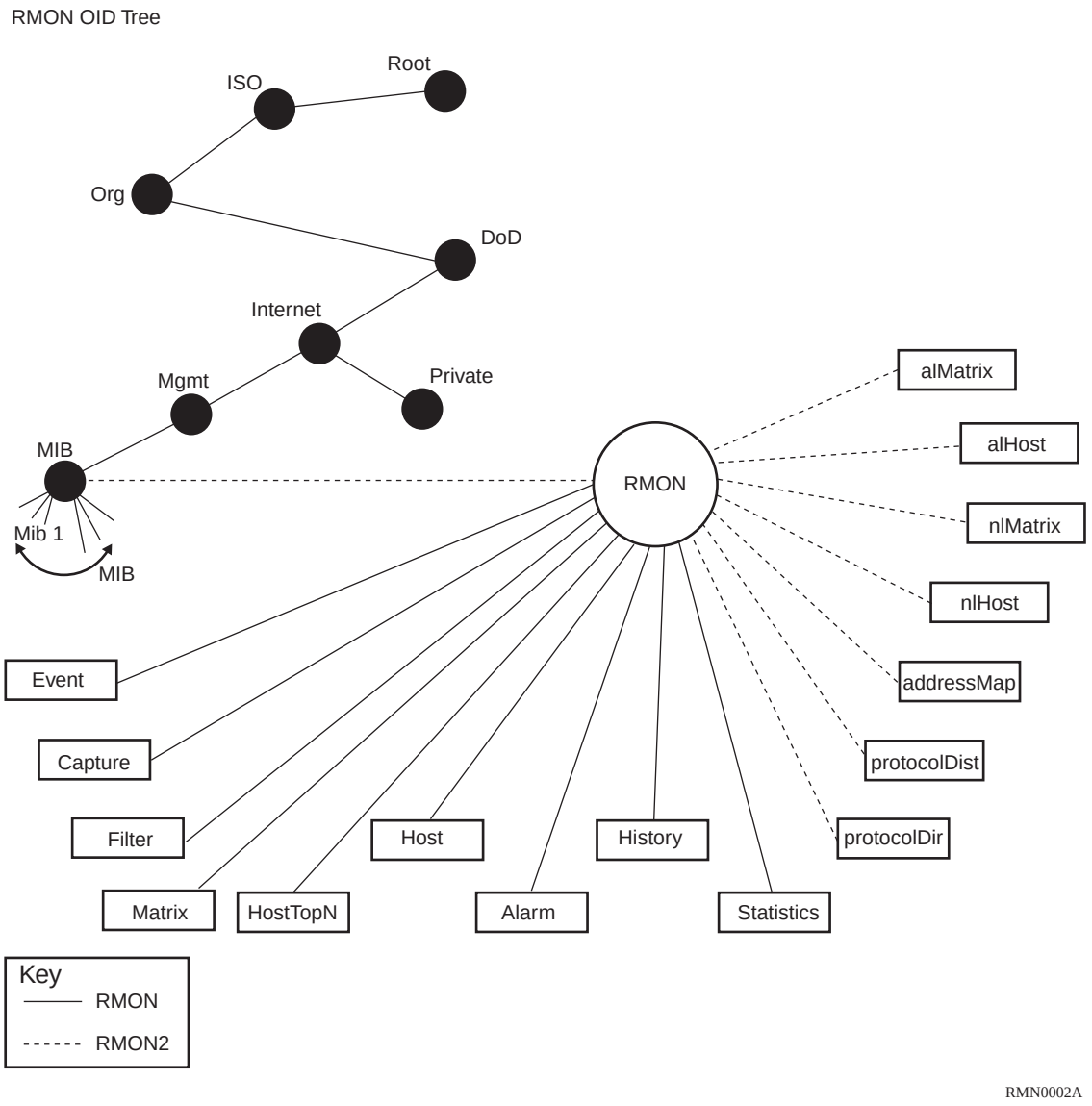

Figure 1-2. RMON/RMON2 MIB Tree

RMON and RMON2 Support on Bay Networks Routers

Table 1-3 summarizes the three levels of RMON and RMON2 support that Bay Networks offers and describes how Bay Networks implements this support.

Table 1-3. Summary of RMON and RMON2 Support

RMON Support	Router Model	Configuration Tasks
RMON alarm and event groups only	All routers (no Ethernet DCM)	You must enable the RMON alarm and event subagent (RAESA) on the router using Technician Interface commands (see *Using Technician Interface Software*). After you enable alarm and event groups on the router, you can configure the Threshold Manager in Optivity LAN to set alarms on any integer-based object in the MIB tree. Then you can configure the Fault Correlator tool in Optivity LAN to receive traps when the threshold is exceeded.
Mini-RMON, which includes built-in RMON capability for the following RMON MIB groups: • Statistics • History • Alarm • Event	ARN 100 (no Ethernet DCM)	Use Site Manager to enable RMON statistics on the ARN 100 base module (see Chapter 3). This action loads the RMONstat subagent, which contains both the statistics and history groups. It also loads the RAESA subagent, which contains the alarm and event groups. Use Optivity Analysis RMON tools (see Table 1-4) to configure, retrieve, and view these RMON statistics.
Complete support for all nine RMON groups and for seven RMON2 groups	• AN/ANH and ARN with Ethernet DCM • ARN 100 with Ethernet expansion module and Ethernet DCM	Using Site Manager or the BCC, you must enable the Ethernet DCM (see Chapter 2). This action enables the following subagents on the router: • Ethernet DCM • DCM middleware (DCMMW) • RAESA Use RMON tools in Optivity Analysis for Windows NT® to configure, retrieve, and view RMON and RMON2 statistics.

For more information about configuring DCM-enabled RMON, see Chapter 2, "Starting RMON and RMON2 on AN/ANH and ARN Routers." For information about configuring mini-RMON on an ARN 100 router, see Chapter 3, "Configuring Mini-RMON on an ARN 100 Router."

RMON and RMON2 Architecture

The Bay Networks RMON and RMON2 architecture consists of the following components:

- AN/ANH and ARN base modules and ARN Ethernet expansion modules, which reside on the router
- DCM, which physically attaches to the router's base module and contains its own flash memory module
- DCM agent software, which operates on the Ethernet DCM
- Data collection module middleware (DCMMW), which operates on the router's base module
- RMON agent software, which operates on the router's base module
- Network management software, which resides on an RMON network management station

The RMON network management station sends SNMP **set** and **get** commands requesting information from the DCM agent that resides on the Ethernet DCM on the router. The RMON agent sends the requested information to the network management station, which then processes and displays this information on its console.

Figure 1-3 illustrates the components of this architecture. The sections that follow describe them in more detail.

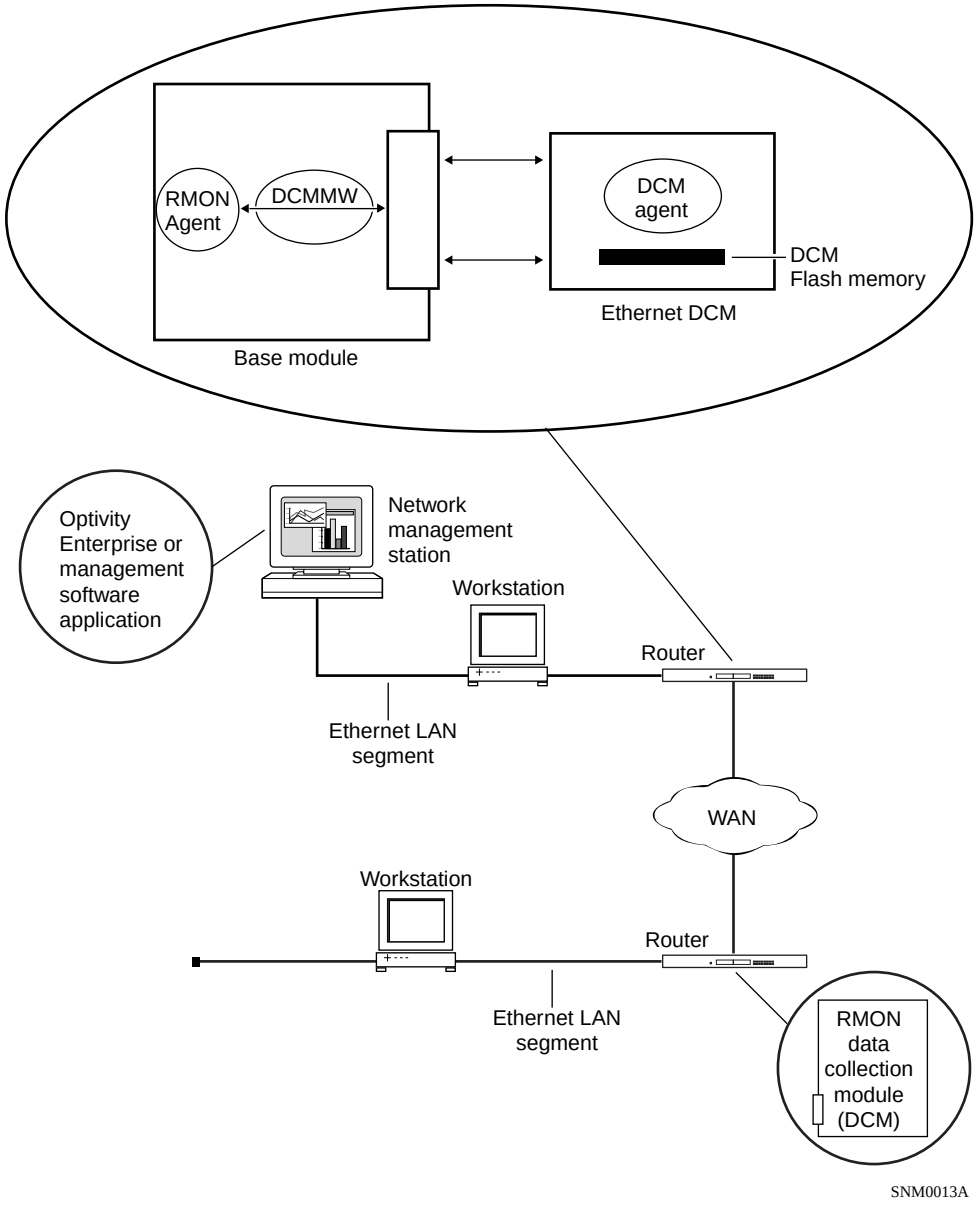

Figure 1-3. RMON/RMON2 Architecture

Data Collection Module (DCM)

The Ethernet DCM, which runs the DCM agent software, physically connects to the BayStack router base module and the ARN Ethernet expansion module. The Ethernet DCM contains a flash memory module for its own boot image and configuration files.

DCM Agent Software

The DCM agent software resides on a DCM installed on an AN/ANH or ARN router. The DCM agent continually collects and analyzes Ethernet data in real time on a single LAN segment (RMON), on groups of LANs (RMON), or on an enterprise network (RMON2). The DCM agent stores the data locally in the Ethernet DCM according to the RMON specification, defined in RFC 1757, or the RMON2 MIB specification, in compliance with RFC 2021.

You can enable multiple DCM agents running on different segments of the network, with a single network management station controlling and accessing them.

DCM Middleware (DCMMW)

To communicate with the DCM software on the Ethernet DCM, the router uses a software subsystem, the DCM middleware (DCMMW). This software subsystem enables and configures an installed Ethernet DCM and allows you to modify the Ethernet DCM configuration, boot the Ethernet DCM, download the DCM image from the base module to the Ethernet DCM, and disable the Ethernet DCM using Site Manager or the BCC. You can use an SNMP-based network management application that supports RMON to view RMON and RMON2 statistics.

RMON Agent Software

The RMON agent software resides on the router's base module and supports the alarm and event groups on all Bay Networks routers. The RMON agent software also supports the statistics and history groups on the ARN 100 router and communicates with the DCMMW software subsystem to access RMON and RMON2 data collected by the Ethernet DCM.

RMON Network Management Software

An RMON network management software application, also known as a *client*, runs on a network management station, which can be a workstation or PC running UNIX or Windows®. Many RMON clients located at various locations can simultaneously retrieve information from an AN/ANH or ARN router located on a specific LAN segment within an internetwork. Optivity Analysis for Windows NT® is an example of an RMON network management application.

After you enable the Ethernet DCM on a router and the Ethernet DCM is collecting statistics, you can use the following network management applications to view, analyze, and monitor network RMON and RMON2 statistics:

- Optivity Analysis for UNIX and Optivity LAN applications, which are part of the Optivity Enterprise™ network management suite
- Optivity Analysis for Windows NT

Optivity Analysis for UNIX

Optivity Analysis for UNIX is a set of graphical network management applications based on RMON. These Optivity® applications offer powerful RMON-based tools that let you view statistics for an enterprise-wide internetwork, for specific LAN segments within an internetwork, or for hosts on a LAN segment.

Each RMON tool is a complete application that represents an intelligent implementation of the RMON and RMON2 MIB groups. After the tool requests and receives information from the network management station, it processes the information and displays a graphical summary of network traffic. Each tool is configurable, so you can obtain exactly the type of information you need.

In Optivity Analysis, the RMON tools provide methods for collecting data for all RMON and RMON2 MIB groups. Table 1-4 summarizes the RMON-based tools and lists the corresponding RMON MIB groups that they use to collect and display traffic statistics.

Table 1-4. Optivity Analysis for UNIX RMON-Based Tools

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Segment Statistics	Display and record information from the RMON statistics group. This information includes raw packet counts and bandwidth utilization.	Plan bandwidth-intensive tasks. Baseline individual segment traffic characteristics.	Ability to view multiple sessions Automatic utilization calculation based on available bandwidth History collection	Statistics
Host Statistics	Display traffic summaries for each host on a selected segment. Provide a HostTopN filter that allows you to concentrate on only the most active hosts on the network.	Determine which hosts are generating specific types of traffic.	Filter for viewing TopN hosts Link packet capture	Host Table and HostTopN
Host Matrix	Present statistics on conversations between host pairs on a selected segment.	Isolate sources of broadcasts, errors, and so forth. Locate workgroups for segmentation.	Sparse matrix display Quick view of graphic coding of information Level 3 support for conversations by protocol	Matrix

(continued)

Table 1-4. Optivity Analysis for UNIX RMON-Based Tools *(continued)*

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Filter/Capture	Define channels and filters. Activate channels for captures.	Capture packets for analysis of a specific problem or to provide selective traffic statistics.	Flexible channel and filter editors Real-time display of counters Automatic capture activation from other tools	Filter and Capture
DecodeMan	Decode and display captured packet content.	Troubleshoot problems by pinpointing the source.	Full seven-layer decode Quick search index Quick configuration of RMON probes for standalone operation	Filter and Capture
Alarm Editor	View thresholds for segment. Run Learning Tool locally.	Modify individual normative models. Run Learning Tool with local configuration for specific segment.	Editing of individual thresholds and hysteresis values interactively	Ancillary to Alarm and Event
Alarm Monitor	Continually monitor all segments.	Proactive maintenance	Monitors all segments at once Quick filter by segment or alarm type Link to Filter/Capture and DecodeMan	Alarm and Event
Protocol Distribution (RMON2)	Provide breakdown by protocol type	Analyze protocols and applications contributing to the overall traffic levels on the network.	N/A	Protocol Distribution

(continued)

Table 1-4. Optivity Analysis for UNIX RMON-Based Tools *(continued)*

Tool Name	Purpose	Possible Uses	Special Features	RMON MIB Group
Network Layer Matrix (RMON2)	View conversation pairs across router boundaries.	Analyze traffic flow to predict bottlenecks and plan for growth.	Shows statistics on traffic between pairs of hosts (in/out, packets, octets, and so forth)	Network Layer Matrix
Learning Tool	Automatically “learn” normal network behavior on all segments.	Create normative model comprising threshold values for all segments.	Learns automatically Flexible sample Builds model statistically	Ancillary to Alarm and Event
TrafficMan	Graphically represent the relationship between end stations, including relative traffic volumes and the primary network layer protocol used.	Identify hosts or conversations that require attention. View statistics for specific hosts and conversations. Start other RMON tools directly from TrafficMan map.	Filters TrafficMan map on a variety of features, including upper-layer protocols such as FTP and HTTP	N/A

For detailed information about how to install, configure, and customize the RMON-based tools for use with RMON and RMON2, see *Using Optivity Analysis 8.x*.

Optivity LAN

Optivity LAN offers two tools you can use to monitor network statistics collected by the RMON agent: Threshold Manager and Fault Correlator. These tools allow you to set thresholds on integer-based objects and display trap information when a threshold is exceeded.

Threshold Manager

After you establish a level of performance that you consider normal for your network, you can configure your system to generate responses whenever your network performance becomes abnormal.

You can also set thresholds that initiate alarms whenever specified network conditions occur. Whenever a threshold is met or exceeded, the specified event occurs and the alarm is triggered. You can set thresholds specific to a slot or port.

For detailed information about installing the Threshold Manager tool, see *Using Optivity LAN 7.1 for UNIX*.

Fault Correlator

After you set alarm thresholds on integer-based variables using the Threshold Manager, you can use the Fault Correlator tool to decode the traps that are sent to the RMON network management station.

The Fault Correlator generates fault reports and calculates the current state of network objects and devices. Optivity LAN automatically stores this information in the Optivity fault database.

For detailed information about using the Fault Correlator tool, see *Using Optivity LAN 7.1 for UNIX*.

Optivity Analysis for Windows NT

Optivity Analysis for Windows NT monitors the performance of heterogeneous LANs to help you identify and solve network problems quickly before they lead to network failure.

Optivity Analysis for Windows NT supports the RMON and RMON2 MIBs and provides a powerful interface that allows you to poll the RMON devices (probes, routers, and switches) on your network. You can poll a device and inquire about errors, bandwidth, and so forth.

Optivity Analysis for Windows NT can monitor hundreds or even thousands of LAN segments by dividing large, complex networks into more manageable domains. Optivity Analysis for Windows NT allows you to view traffic statistics generated from a single LAN, groups of LANs, or an enterprise network.

With Optivity Analysis for Windows NT, you can establish and report on network trends over extended periods and create baselines that set alarms so that an accurate picture of the network can be portrayed.

For more information about using Optivity Analysis for Windows NT, see *Using Optivity Analysis for Windows NT Version 1.x*.

Chapter 2
Starting RMON and RMON2 on AN/ANH and ARN Routers

This chapter lists the requirements for starting RMON and RMON2 using Site Manager and the BCC. It also includes the procedures for configuring RMON and RMON2 on AN/ANH and ARN routers using the default configuration values.

Note: If you want to configure the built-in version of RMON on an ARN 100 router with no Ethernet DCM using Site Manager, go to Chapter 3, "Configuring Mini-RMON on an ARN 100 Router."

This chapter contains the following information:

Topic	Page
Router Hardware and Software Prerequisites	2-2
Starting Configuration Tools	2-4
Starting RMON and RMON2	2-4
Customizing the Ethernet DCM	2-9

For detailed information about RMON and RMON2 and the Bay Networks implementation of RMON and RMON2, see Chapter 1, "RMON and RMON2 Overview."

Router Hardware and Software Prerequisites

Before you can use the full RMON and RMON2 functionality on BayStack AN/ANH, ARN, and ARN 100 routers, your router must meet specific hardware and software requirements.

To ensure a successful implementation of RMON and RMON2, complete the following tasks:

1. **Install an Ethernet DCM module in each BayStack AN/ANH or ARN router from which you want to collect RMON and RMON2 statistics.**

   For complete installation instructions, see one of the following guides:

   - *Installing an N11 Data Collection Module (DCM) in a BayStack AN*
   - *Installing an N11 Data Collection Module (DCM) in an 8-Port ANH*
   - *Installing an Ethernet RMON DCM in a BayStack ARN Router*

2. **Upgrade the memory on the Ethernet DCM. The minimum memory requirements are as follows:**

   - RMON: 4 MB
   - RMON2: 8 MB

   To determine how much memory you need to configure RMON MIB groups and to store the data for these groups, see "Memory Requirements for RMON Groups" on page C-11.

3. **Review the recommended software and hardware requirements for RMON and RMON2 operation.**

   Table 2-1 lists the software and hardware requirements for RMON and RMON2 operation on BayStack AN/ANH routers.

Table 2-1. AN/ANH Requirements for Using RMON and RMON2

Software/Hardware	Recommended Version
DCM hardware	Revision E
Boot PROM	Version 9.00c (*anboot.exe* v9.00c) or later
Diagnostic PROM	Version v7.30 (*andiag.exe* v7.30) or later
BayRS	BayRS Version 12.20 (*an.exe* v12.20) or later
DCM agent software	DCM Agent Software Version 2.00.1 (*in_2.00.1.obj*)

Table 2-2 lists the software and hardware requirements for RMON and RMON2 operation on BayStack ARN routers.

Table 2-2. ARN Requirements for Using RMON and RMON2

Software/Hardware	Recommended Version
DCM hardware	Revision E
Boot PROM	Version 1.19 (*arnboot.exe* v1.19) or later
Diagnostic PROM	Version 2.00 (*arndiag.exe* v2.00) or later
BayRS	Version 12.20 (*arn.exe* v12.20) or later
DCM agent software	Version 2.00.1 (*in_2.00.1.obj*)

Caution: Enabling an Ethernet DCM with DCM agent software earlier than Version 2.00.1 generates a warning log message, which prevents the Ethernet DCM from booting successfully.

4. **Verify minimum DCM requirements to determine whether you need to upgrade the DCM software image on the router.**

   For instructions, see Appendix D, "Upgrading the DCM Software Image."

5. **Configure an Ethernet interface for each LAN segment you want to monitor.**

6. **Install and configure on your network management station one of these network management applications to view and analyze RMON and RMON2 statistics generated by the Ethernet DCM:**

   - Optivity Enterprise (contains Optivity Analysis for UNIX and Optivity LAN)
   - Optivity Analysis for Windows NT

Starting Configuration Tools

Before configuring RMON and RMON2, see the appropriate user guide for instructions on how to start and use the Bay Networks configuration tool of your choice.

Configuration Tool	User Guide
Bay Command Console (BCC™)	*Using the Bay Command Console*
Site Manager	*Configuring and Managing Routers with Site Manager*

These guides also describe generally how to create and modify a device configuration.

Starting RMON and RMON2

To begin using RMON and RMON2 for data collection on BayStack routers, you must enable the Ethernet DCM using the default configuration.

To start RMON and RMON2 on Ethernet DCM-enabled AN/ANH and ARN routers using the BCC or Site Manager, perform the following tasks:

- Prepare a configuration file.
- Configure the Ethernet DCM.

Preparing a Configuration File

To create a configuration file using Site Manager, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. From the Site Manager main menu, choose **Tools.**	The Tools menu opens.
2. Choose **Configuration Manager.**	The Configuration Manager window opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
3. Choose **Local File**, **Remote File**, or **Dynamic.**	Site Manager prompts you to choose a configuration file.
4. Select the configuration file and click on **OK**.	The Configuration Manager window opens, displaying the router models.

For information about Site Manager and how to work with configuration files, see *Configuring and Managing Routers with Site Manager.*

Configuring an Ethernet DCM for AN/ANH Routers

Before you can configure an Ethernet DCM on an AN/ANH router, you must configure IP and SNMP on the router (see *Configuring SNMP, BootP, DHCP, and RARP Services*.)

When you configure the Ethernet DCM for an AN/ANH router, you create the DCM middleware (DCMMW) configuration using the default parameter values. For information about modifying the default values, see Chapter 4, "Customizing a DCM for RMON and RMON2."

For an AN/ANH router, you can only configure a DCM base module.

Using the BCC

To configure an Ethernet DCM for an AN/ANH router:

1. **Navigate to the root (box) level and enter RMON configuration mode:**

   rmon

2. **Set the module type for the DCM that you want to configure by entering:**

   dcm dcm-id *<module>*

   Module is either base-module or expansion-module.

For example, the following command line configures the DCM base-module on an AN router:

```
rmon# dcm dcm-id base-module
dcm/base-module#
```

The following command line configures the DCM expansion-module on an ARN router:

```
rmon# dcm dcm-id expansion-module
dcm/expansion-module#
```

Using Site Manager

To configure an Ethernet DCM for an AN/ANH router, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose the AN router model.	
2. Click on **Confirm.**	
3. Choose a net module for the DCM, for example, 8pt. EHub/3S/N11/DCM, then click on **OK**.	
4. Choose the link or net module connector on which you are configuring the Ethernet DCM, for example, XCVR, then click on **OK**.	The Select Protocols window opens.
5. Choose **IP**, then click on **OK**.	The IP Configuration window opens.
6. Click on **OK**.	You return to the Configuration Manager window.
7. Choose **Platform**.	The Platform menu opens.
8. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
9. Choose **Create Base Module DCM**.	The Edit Base Module DCM Parameters window opens.
10. Click on **OK** to accept the default configuration parameters.	You return to the Configuration Manager window.

When you enable the Ethernet DCM, the RMON Object Support parameter is set to RMON2 by default, allowing the Ethernet DCM to collect both RMON and RMON2 statistics. You can use Optivity Analysis for UNIX or Optivity Analysis for Windows NT to view and analyze RMON and RMON2 statistics.

Configuring an Ethernet DCM for ARN Routers

Before you can configure an Ethernet DCM on an ARN router, you must configure IP and SNMP on the router (see *Configuring SNMP, BootP, DHCP, and RARP Services*).

When you configure the Ethernet DCM for an ARN router, you create the DCM middleware (DCMMW) configuration using the default parameter values. For information about modifying the default values, see Chapter 4, "Customizing a DCM for RMON and RMON2."

For an ARN router, you can configure up to two DCMs: one on the router's base module and one on the router's expansion module. You must configure each module separately.

Using the BCC

To configure an Ethernet DCM for an ARN router:

1. **Navigate to the root (box) level and enter RMON configuration mode:**

   rmon

2. **Set the module type for the DCM that you want to configure by entering:**

   dcm dcm-id <*module_type***>**

   Module_type is either base-module or expansion-module.

   For example, the following command sequence configures one DCM on an ARN router base module and another DCM on an ARN router expansion module:

```
rmon# dcm dcm-id base-module
dcm/base-module# dcm dcm-id expansion-module
dcm/expansion-module#
```

Using Site Manager

To configure an Ethernet DCM for an ARN router, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose an ARN router model.	
2. Click on **Confirm.**	
3. Choose the base, expansion, or adapter module you want to configure for the ARN router. You must choose each module separately. For example: • For a base module, choose **Ethernet**. • For an expansion module, choose **Ethernet DCM**. • For an adapter module, choose **ISDN 'V.'**	
4. Click on **OK**.	
5. Choose a net or link module for the ARN router.	
6. Choose the link or net module connector on which you are configuring the Ethernet DCM.	The Add Circuit window opens.
7. Accept the default circuit name or modify it, then click on **OK**.	The Select Protocols window opens.
8. Choose **IP**, then click on **OK**.	The IP Configuration window opens.
9. Click on **OK**.	You return to the Configuration Manager window.
10. Choose **Platform**.	The Platform menu opens.
11. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
12. Choose **Create Base Module DCM** or **Create Expansion Module DCM**. You can enable a DCM on both an Ethernet base module and an Ethernet expansion module with an installed DCM.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
13. Click on **OK** to accept the default configuration parameters.	You return to the Configuration Manager window.

When you enable the Ethernet DCM, the RMON Object Support parameter is set to RMON2 by default, allowing the Ethernet DCM to collect both RMON and RMON2 statistics. You can use Optivity Analysis for UNIX or Optivity Analysis for Windows NT to view and analyze RMON and RMON2 statistics.

Customizing the Ethernet DCM

For information about customizing the DCMMW configuration parameters, see Chapter 4, “Customizing a DCM for RMON and RMON2.”

Chapter 3
Configuring Mini-RMON on an ARN 100 Router

On the ARN 100 router, Bay Networks provides a condensed version of the RMON MIB standard, called *mini-RMON*. Mini-RMON supports the following four RMON MIB groups:

- Statistics
- History
- Alarm
- Event

Unlike the AN/ANH and ARN routers, which use an installed Ethernet DCM to collect RMON statistics, the ARN 100 router contains built-in RMON capability on the router's base module. Using Site Manager to configure the ARN 100 base module, you can enable the ARN 100 to collect RMON statistics.

After you configure the ARN 100 router to collect RMON statistics, you can view these statistics using the RMON tools in Optivity Analysis for UNIX or Optivity Analysis for Windows NT. For information about using these RMON tools, see "RMON Network Management Software" on page 1-12.

Configuration Considerations

If you choose, you can upgrade an ARN 100 router to collect complete RMON and RMON2 statistics by installing an Ethernet expansion module on the router's base module and attaching the Ethernet DCM to it. You can collect full RMON/RMON2 statistics only from the segment attached to the router's Ethernet expansion module.

You cannot collect RMON statistics from both the base module and the Ethernet DCM (full RMON/RMON2). This restriction is enforced in the following way for ARN 100 routers:

- If you enable the DCMMW subsystem on an ARN 100 router and then configure mini-RMON on the ARN 100 base module, the DCMMW subsystem is disabled. (DCMMW is unloaded and its load mask is cleared.)
- If you enable mini-RMON on the base module and you then configure the DCMMW subsystem, mini-RMON is disabled. (Mini-RMON is unloaded and its load mask is cleared.)

For information about installing an Ethernet DCM on an Ethernet expansion module in an ARN router, see *Installing an Ethernet RMON DCM in a BayStack ARN Router*. For information about starting RMON and RMON2 on an ARN 100 router with an installed Ethernet DCM, see Chapter 2, "Starting RMON and RMON2 on AN/ANH and ARN Routers."

Starting Mini-RMON

To start RMON data collection on an ARN 100 base module, use Site Manager to perform the following tasks:

- Prepare a configuration file.
- Enable the base module and RMON data collection.

Preparing a Configuration File

To create a configuration file, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. From the Site Manager main window, choose **Tools.**	The Tools menu opens.
2. Choose **Configuration Manager.**	The Configuration Manager window opens.
3. Choose **Local File**, **Remote File**, or **Dynamic.**	Site Manager prompts you to choose a configuration file.
4. Select the configuration file and click on **OK**.	The Configuration Manager window opens, displaying the router models.

For information about Site Manager and how to work with configuration files, see *Configuring and Managing Routers with Site Manager.*

Enabling Mini-RMON Data Collection

To begin collecting mini-RMON statistics on the ARN 100 base module, you enable the base module and then enable RMON by completing the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose the ARN router model.	
2. Click on **Confirm.**	
3. Choose the 10/100BASE-TX Ethernet or the 100BASE-FX Ethernet net or link module for the ARN 100 router.	
4. Click on **OK.**	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
5. Choose the link or net module connector on which you are enabling mini-RMON, for example, XTRCV.	The Add Circuit window opens.
6. Accept the default circuit name or modify it, then click on **OK**.	The Select Protocols window opens.
7. Choose **IP** and **RIP**, then click on **OK**.	
8. Set the following parameters: • **IP Address** • **Subnet Mask** • **Transmit Bcast Addr** • **UnNumbered Assoc Address** Click on **Help** or see *Configuring IP Services* for parameter descriptions.	
9. Click on **OK**.	You return to the Configuration Manager window.
10. Choose **Platform**.	The Platform menu opens.
11. Choose **RMON Stats 12.10 and later.**	The RMON Stats 12.10 and later menu opens.
12. Choose **Enable Base Module RMON Stats.**	The Enable Base Module RMON Stats menu opens, indicating that you have enabled the base module for RMON data collection.

Disabling Mini-RMON Data Collection

To stop collecting mini-RMON statistics on the Ethernet, you must delete the RMON Stats base module on the ARN 100 router.

To delete the RMON Stats base module on the ARN 100 router, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **RMON Stats 12.10 and later.**	The RMON Stats 12.10 and Later menu opens.
3. Choose **Delete Base Module RMON Stats**.	The Configuration Manager disables data collection by deleting the base module on the ARN 100.

Chapter 4
Customizing a DCM for RMON and RMON2

This chapter describes how to customize the configuration of an Ethernet DCM by editing the DCMMW parameters. It contains the following information:

Topic	Page
Disabling the Ethernet DCM	4-2
Specifying RMON or RMON2 Data Collection	4-3
Specifying the Configuration Mode	4-6
Saving the Configuration Information	4-7
Configuring the DCM Image on the Router	4-9
Modifying Default RMON MIB Group Parameters	4-12
Rebooting the Ethernet DCM	4-18
Deleting the Ethernet DCM Software Subsystem	4-19
Using the Technician Interface to Manage a DCM	4-20

For detailed information about RMON and RMON2 and the Bay Networks implementation of RMON and RMON2, see Chapter 1, "RMON and RMON2 Overview." For a description of all Ethernet DCM parameters, see Appendix B, "Ethernet DCM Parameters."

Disabling the Ethernet DCM

By default, DCM data collection is enabled on the router. Before you can modify DCMMW configuration parameters for an installed Ethernet DCM, you must temporarily disable the Ethernet DCM from collecting data. When you finish modifying the DCMMW configuration parameters, you must reenable the Ethernet DCM for these changes to take effect.

Using the BCC

To temporarily disable the DCM from collecting data, navigate to the dcm/base-module context or the dcm/expansion-module context (for example, **box; dcm/base-module**) and enter:

state disabled

For example, the following command line disables DCM data collection on the base-module of an AN/ANH router:

```
dcm/base-module# state disabled
dcm/base-module#
```

The following command line disables DCM data collection on the expansion-module of an ARN router:

```
dcm/expansion-module# state disabled
dcm/expansion-module#
```

Using Site Manager

To temporarily disable the DCM from collecting data, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global**.	The Global menu opens.
4. Choose one of the following options: • **Base Module DCM** • **Expansion Module DCM**	If you choose **Base Module DCM,** the Edit Base Module DCM Parameters window opens. If you choose **Expansion Module DCM** for an ARN router, the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.

Specifying RMON or RMON2 Data Collection

When you enable one Ethernet DCM using Site Manager default values, the DCM collects RMON2 and RMON statistics from the AN/ANH or ARN router. Although the ARN router supports two Ethernet DCMs, it cannot collect RMON2 statistics from more than one Ethernet DCM simultaneously.

When you enable one Ethernet DCM using BCC default values, the DCM collects only RMON statistics. You can configure the DCM to collect both RMON and RMON2 statistics, but only on one DCM.

You can specify which Ethernet DCM you want to collect RMON2 statistics from; any additional Ethernet DCMs automatically default to RMON.

Using the BCC

To specify the Ethernet DCM from which you want to collect RMON and RMON2 statistics or just RMON statistics, navigate to the rmon-control context (for example, **box; rmon/dcm dcm-id base-module/rmon-control**) and enter:

rmon2 level *<statistics>*

Statistics is either rmon or rmon2.

For example, the following command sequence specifies the Ethernet DCM that collects RMON2 statistics and displays the object support level:

```
rmon-control/base-module# rmon2 level rmon2
rmon2/base-module# info
level rmon2
```

The following command sequence specifies that the Ethernet DCM collects both RMON and RMON2 statistics and display the object support level:

```
rmon2/base-module# rmon2 level rmon
rmon2/base-module# info
level rmon
```

Using Site Manager

To specify the Ethernet DCM from which you want to collect RMON2 statistics, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM.**	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **RMON Object Support** parameter. Click on **Help** or see the parameter description on page B-6.	
9. Set the **Enable/Disable** parameter to **Enable.** Click on **Help** or see the parameter description on page B-2.	
10. Click on **OK**.	You return to the Configuration Manager window.

Specifying the Configuration Mode

By default, the Ethernet DCM uses the configuration file in its own local flash memory. If you want to use the configuration information in the DCM DRAM, written by DCMMW from the BayStack router's file system, set the Configuration Mode parameter to shared memory. Shared memory is the area on the Ethernet DCM through which the router's base module and the Ethernet DCM exchange information.

Using the BCC

To specify whether you want to use the configuration information in DCM DRAM or in DCM flash memory, navigate to the dcm/base-module context or the dcm/expansion-module context (for example, **box; dcm/base-module**) and enter:

config-mode <*mode_type***>**

Mode_type is either probe-memory (local) or shared-memory.

For example, the following command lets you access the configuration information in DCM DRAM:

```
dcm/base-module# config-mode shared-memory
dcm/base-module#
```

The following command lets you access the configuration information in DCM flash memory:

```
dcm/base-module# config-mode probe-memory
dcm/base-module#
```

Using Site Manager

To specify the configuration mode, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Configuration Mode** parameter. Click on **Help** or see the parameter description on page B-4.	
9. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see page B-2.	
10. Click on **OK**.	You return to the Configuration Manager window.

Saving the Configuration Information

By default, the DCM saves the configuration information in DRAM to its local DCM flash memory (overwriting the existing configuration file). If you do not want to overwrite the DCM configuration file in flash memory, configure the DCM so that it does not save the configuration information.

Using the BCC

To set the save mode for the configuration information, navigate to the dcm/base-module or expansion-module context (for example, **box; dcm/base-module**) and enter:

save-mode <*mode***>**

Mode is either save (default) or no-save.

For example, the following command line specifies that the DCM uses the configuration file in its local flash memory but does not save the configuration information in its local flash memory:

```
dcm/base-module# config-mode probe-memory save-mode no-save
dcm/base-module#
```

The following command specifies that the DCM uses the configuration file in DCM DRAM and saves the configuration information in DRAM to its local flash memory:

```
dcm/base-module# config-mode shared-memory save-mode save
dcm/base-module#
```

Using Site Manager

To set the save mode for the configuration information, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Configuration Mode** parameter. Click on **Help** or see the parameter description on page B-4.	
9. Set the **Save Configuration Info** parameter. Click on **Help** or see the parameter description on page B-4.	
10. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
11. Click on **OK**.	You return to the Configuration Manager window.

Configuring the DCM Image on the Router

You configure the DCM image on the router by specifying the following required parameters:

- By default, the DCM uses the image file in its local flash memory as the DCM boot image. The boot image option, which specifies whether the DCM boots with the image file in its local flash memory (local) or with a boot image copied from the router's flash memory card (download).
- The router volume and file name for the image you want the DCM to boot. The boot image name cannot exceed 255 characters.
- The image save mode, which specifies whether or not the DCM saves the active DCM image to its local flash memory.

  By default, the DCM saves the boot image file in DRAM to its local flash memory (overwriting the existing image file). You can choose not to save the DCM boot image file (the image remains in DRAM until the next time the DCM boots).

Using the BCC

Before you can configure the DCM boot image on the router, make sure that the **config-mode** parameter is set to shared-memory. Then configure the DCM boot image by specifying an explicit value for the following required parameters: **image-name, boot-option**, and **save-mode**.

To configure the DCM boot image on the router, navigate to the dcm/base-module or dcm/expansion-module context (for example, **box; dcm/expansion-module**) and enter the following required parameters:

image image-name *<volume_number:filename>* **boot-option** *<option>* **save-mode** *<mode>*

Volume_number:filename is the volume and the file name of the image that you want the DCM to boot.

Option is either local or download.

Mode is either save or no-save.

For example, the following command sequence sets the config-mode parameter to shared-memory, then specifies that the DCM boots with the image file *11_140.obj* on volume 1 of the router's flash memory (**download**) and saves the DCM image in the DCM flash memory:

```
image/base-module# image image-name 1:11_140.obj boot-option download
save-mode save
image/base-module#
```

Using Site Manager

To configure the DCM boot image on the router, complete the tasks in the following table:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Boot Option** parameter. Click on **Help** or see the parameter description on page B-2.	
9. Set the **Image Name** parameter. Click on **Help** or see the parameter description on page B-3.	
10. Set the **Image Save Mode** parameter. Click on **Help** or see the parameter description on page B-3.	
11. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
12. Click on **OK**.	You return to the Configuration Manager window.

Modifying Default RMON MIB Group Parameters

If necessary, you can change the default values for the following RMON MIB group parameters:

- Maximum number of host addresses collected in each RMON host control table
- Whether the DCM creates the RMON host control table when it boots
- Whether the DCM creates the RMON matrix control table when it boots

For more information about the RMON host control and matrix control tables, see "RMON MIB Group Controls and Functions" on page C-2.

Go to the sections that follow to set these RMON MIB group parameters.

Specifying the Maximum Number of RMON Hosts

You can specify the maximum number of host addresses to be collected in each RMON host control table. The maximum limit depends on the amount of flash memory available in the DCM. When the host control table reaches the maximum value, the DCM deletes entries based on an LRU (least recently used) algorithm.

Using the BCC

To specify the maximum number of host addresses to be collected in the RMON matrix control table, navigate to the rmon-control/base-module or rmon-control/expansion-module context (for example, **box; rmon-control/ base-module**) and enter:

max-hosts <*integer***>**

Integer is the maximum number of host addresses that the DCM collects and stores in the RMON host control table. Host addresses range from 100 through 8128.

For example, the following command line sets the maximum number of hosts in the RMON control table to 300:

```
rmon-control/base-module# max-hosts 300
rmon-control/base-module#
```

Using Site Manager

To specify the maximum number of RMON hosts, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window opens or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window opens or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Configuration Mode** parameter to **Shared Memory**. Click on **Help** or see the parameter description on page B-4.	
9. Set the **RMON Max Host** parameter. Click on **Help** or see the parameter description on page B-5.	
10. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
11. Click on **OK**.	You return to the Configuration Manager window.

To verify the number of hosts configured, check the MIB object wfDCMmsRMONHost using the Site Manager Statistics tool.

Enabling and Disabling the RMON Host Control Table

By default, the DCM does not create the RMON host control table when it boots. If your RMON network management application does not enable and disable its own host configuration during normal operation, you may need to enable the DCM to create it.

The DCM allows only one instance of the host control table.

Using the BCC

To enable the creation of the RMON host control table, navigate to the rmon-control/base-module or rmon-control/expansion-module context (for example, **box; rmon-control/expansion-module**) and enter:

host-control enabled

For example, the following command line enables the creation of the RMON host control table, allowing the DCM to create default host entries in this table:

```
rmon-control/expansion-module# host-control enabled
rmon-control/expansion-module#
```

To disable the creation of the RMON host control table, navigate to the rmon-control/base-module or rmon-control/expansion-module context (for example, **box; rmon/rmon-control/expansion-module**) and enter:

host-control disabled

For example, the following command line disables the RMON host control table, preventing the DCM from creating default host entries in this table:

```
rmon-control/expansion-module# host-control disabled
rmon-control/expansion-module#
```

Using Site Manager

To enable or disable the creation of the RMON host control table, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Configuration Mode** parameter to **Shared Memory**. Click on **Help** or see the parameter description on page B-4.	
9. Set the **RMON Default Host** parameter. Click on **Help** or see the parameter description on page B-5.	
10. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
11. Click on **OK**.	You return to the Configuration Manager window.

Enabling and Disabling the RMON Matrix Control Table

By default, the DCM does not create the RMON matrix control table when it boots. If your RMON network management application does not enable and disable its own matrix configuration during normal operation, you may need to enable the DCM to create it.

The DCM allows only one instance of the matrix control table.

Using the BCC

To enable the creation of the RMON matrix control table, navigate to the rmon-control/base-module or rmon-control/expansion-module context (for example, **box; rmon-control/expansion-module**) and enter:

matrix-control enabled

For example, the following command line enables the creation of the RMON matrix control table, allowing the DCM to create default matrix entries in this table:

```
rmon-control/expansion-module# matrix-control enabled
rmon-control/expansion-module#
```

To disable the creation of the RMON matrix control table, navigate to the rmon-control context and enter:

matrix-control disabled

For example, the following command line disables the creation of the RMON matrix control table, preventing the DCM from creating default matrix entries in this table:

```
rmon-control/expansion-module# matrix-control disabled
rmon-control/expansion-module#
```

Using Site Manager

To enable or disable the creation of the RMON matrix control table, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Disable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.
7. Repeat steps 1 through 4; then go to step 8.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
8. Set the **Configuration Mode** parameter to **Shared Memory**. Click on **Help** or see the parameter description on page B-4.	
9. Set the **RMON Default Matrix** parameter. Click on **Help** or see the parameter description on page B-6.	
10. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
11. Click on **OK**.	You return to the Configuration Manager window.

Rebooting the Ethernet DCM

After you finish modifying Ethernet DCM configuration parameters, you must reboot the Ethernet DCM for these changes to take effect. You do this by reenabling the Ethernet DCM.

Using the BCC

To reenable the DCM for data collection, navigate to the dcm/base-module or dcm/expansion-module context (for example, **box; dcm/base-module**) and enter:

state enabled

For example, the following command line reenables a DCM to begin collecting data:

```
dcm/base-module# state enabled
dcm/base-module#
```

Using Site Manager

To reboot the Ethernet DCM, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and Later menu opens.
3. Choose **Global.**	The Global menu opens.
4. Choose **Base Module DCM** or **Expansion Module DCM**.	The Edit Base Module DCM Parameters window or the Edit Expansion Module DCM Parameters window opens.
5. Set the **Enable/Disable** parameter to **Enable**. Click on **Help** or see the parameter description on page B-2.	
6. Click on **OK**.	You return to the Configuration Manager window.

Deleting the Ethernet DCM Software Subsystem

The router requires the DCMMW software to communicate with the Ethernet DCM. Deleting DCMMW deactivates the Ethernet DCM.

Note: Before you delete the DCMMW, always try disabling the Ethernet DCM first.

Using the BCC

To deactivate the Ethernet DCM, navigate to the dcm/base-module or expansion-module context (for example, **box; dcm/base-module**) and enter:

delete

For example, the following command deactivates the Ethernet DCM on a router:

```
dcm/base-module# delete
rmon#
```

Using Site Manager

To deactivate the Ethernet DCM, complete the following steps:

Site Manager Procedure	
You do this	**System responds**
1. In the Configuration Manager window, choose **Platform**.	The Platform menu opens.
2. Choose **DCM 11.0 and later**.	The DCM 11.0 and later menu opens.
3. Choose **Delete DCM.**	The Delete DCM menu opens.

(continued)

Site Manager Procedure *(continued)*	
You do this	**System responds**
4. Choose one of the following options: • **Base Module DCM only** • **Expansion Module DCM only** • **All DCMs** **Base Module DCM only** removes the DCMMW from the base module on the current platform. **Expansion Module DCM only** removes the DCMMW from the ARN Ethernet expansion module. **All DCMs** removes the DCMMW from all modules on the current platform.	Site Manager displays a confirmation prompt.
5. Click on **OK**.	Site Manager completely deactivates all Ethernet DCMs.

If you need to reactivate the Ethernet DCM after deleting the DCMMW, see "Starting RMON and RMON2" on page 2-4.

Using the Technician Interface to Manage a DCM

You can use Technician Interface commands to:

- Download a new Ethernet DCM software image.

  See Appendix D, "Upgrading the DCM Software Image."

- Display or modify DCMMW configuration parameters.

  See *Using Technician Interface Software* for information about accessing the DCM MIB using **set, get,** and **commit** commands with the MIB object ID.

Caution: The Technician Interface does not verify that the value you enter for a parameter is valid. Entering an invalid value can corrupt your configuration.

- Enable, disable, and reboot the Ethernet DCM.

  See *Using Technician Interface Software* for information about using the **enable/disable dcmmw** scripts.

Caution: Avoid running scripts that continually issue Technician Interface commands while you are running another RMON network management application. This combination can cause the SNMP agent to fill the system buffers with RMON data, causing a system restart.

Appendix A
Monitoring the DCM
Using the BCC show Command

This appendix describes how to use the BCC **show** command to obtain DCM configuration, interface, and statistical information from the management information base (MIB). The type and amount of data displayed depend on the specific DCM settings you want to view.

This chapter includes descriptions of the **show rmon dcm** command.

Note: Enter all commands using lowercase letters.

show rmon dcm

The **show rmon dcm** *<option>* command displays configuration, status, and statistical information about the DCM configured on an AN/ANH or ARN router.

The **show rmon dcm** command supports the following subcommand options

- summary
- image
- dcmconfig
- rmonconfig

summary

Displays configuration and statistical information about all Ethernet DCMs configured on the router.

The output includes the following information:

Data Collection Module #	Number that corresponds to either a base module (1) or an expansion module (2).
DCM State	State of the DCM: enabled or disabled.
Operational Status	Indicates the status of the DCM: up or down.
RMON Object Support	Indicates whether the Ethernet DCM is collecting RMON or RMON2 statistics.
Module Type	Type of circuit to which the DCM is attached on the AN/ANH or ARN router base module or ARN expansion module. The only module type supported by the DCM is Ethernet.
Memory Size	Total size of available memory on the DCM.
Hardware Revision	Revision number associated with the DCM hardware.
Firmware Revision	Revision number associated with the DCM firmware.
Agent Image Version	Version number of the DCM agent software.
Boot Option	Indicates whether the DCM uses the image file in its own flash memory (local) for booting or a boot image copied from the AN/ANH or ARN router's flash memory card to DCM shared memory (download).
Image Name	Name of the image file on the AN/ANH or ARN router's flash memory card.

Image Save Mode	Indicates that the DCM saves the active image to its local flash memory (save) or that the DCM does not save the DCM boot image (no save), if the save mode is no save.
Config Source	Indicates that the DCM uses the default configuration information in the DCM local flash memory (local) or the router's flash memory, stored in DCM DRAM (shared).
Config Save Mode	Indicates that the DCM saves the configuration information to its local flash memory (save) or that the DCM does not save the DCM configuration information (no save).
Max hosts per entry	Maximum number of host addresses to be collected in each entry of the RMON host control table. Addresses range from 100 through 8128.
Configured hosts per entry	Configured number of hosts in each RMON host control entry on the DCM.
Create Host Control Table	Indicates whether the creation of the RMON host control table is enabled or disabled.
Create Matrix Control Table	Indicates whether the creation of the RMON matrix control table is enabled or disabled.

image

Displays information about the DCM image for all Ethernet DCMs configured on the AN/ANH or ARN router, including agent image version, boot option, image name, and image save mode.

The output includes the following information:

Data Collection Module #	Number that corresponds to either a base module (1) or an expansion module (2).
Agent Image Version	Version number of the DCM agent software.
Boot Option	Indicates that the DCM uses the image file in its own flash memory (local) for booting or a boot image copied from the AN/ANH and ARN router's flash memory card to DCM shared memory (download).
Image Name	Name of the image file on the AN/ANH or ARN router's flash memory card.
Image Save Mode	Indicates that the DCM saves the active image to its local flash memory (save) or that the DCM does not save the DCM boot image (no save, if the save mode is nosave.

dcmconfig

Displays configuration information about all Ethernet DCMs configured on the AN/ANH or ARN router, including the state of the DCM, its operational status, its hardware and firmware revisions, and so forth.

The output includes the following information:

Data Collection Module #	Number that corresponds to either a base module (1) or an expansion module (2).
DCM State	State of the DCM: enabled or disabled.
Operational Status	Indicates the operational status of the DCM: up or down.
Module Type	Type of circuit to which the DCM is attached on the AN/ANH or ARN router base module or ARN expansion module. The only module type supported by the DCM is Ethernet.
Memory Size	Total memory size of the DCM software.
Hardware Revision	Revision number associated with the DCM hardware.
Firmware Revision	Revision number associated with the DCM firmware.
Config Source	Indicates that the DCM uses the default configuration information in the DCM local flash memory (local) or the router's flash memory, stored in DCM DRAM (shared).
Config Save Mode	Indicates whether the DCM saves the configuration information to its local flash memory (save) or that the DCM does not save the DCM configuration information (no save).

dcm rmonconfig

Displays information specific to the RMON default configuration, including maximum number of hosts per entry, configured number of hosts per entry, and the status of the host control table and matrix control table.

The output includes the following information:

Data Collection Module #	Number that corresponds to either a base module (1) or an expansion module (2).
RMON Object Support	Indicates whether the Ethernet DCM is collecting RMON or RMON2 statistics.
Max hosts per entry	Maximum number of host addresses collected in each entry of the RMON host control table.
Configured hosts per entry	Configured number of hosts in each RMON host control entry on the DCM.
Create Host Control Table	Indicates whether the creation of the RMON host control table is enabled or disabled.
Create Matrix Control Table	Indicates whether the creation of the RMON matrix control table is enabled or disabled.
Config Save Mode	Indicates whether creation of the DCM saves the configuration information to its local flash memory (save) or that the DCM does not save the DCM configuration information (no save).

Appendix B
Ethernet DCM Parameters

This appendix contains reference information about customizing the parameters for the Ethernet DCM to support RMON and RMON2. For each parameter, this appendix provides the following information:

- Parameter name
- Configuration Manager menu path
- Default setting
- Valid parameter options
- Parameter function
- Instructions for setting the parameter
- Management information base (MIB) object ID

The Technician Interface allows you to modify parameters by issuing **set** and **commit** commands with the MIB object ID. This process is equivalent to modifying parameters using Site Manager. For more information about using the Technician Interface to access the MIB, refer to *Using Technician Interface Software*.

Caution: The Technician Interface does not verify the validity of your parameter values. Entering an invalid value can corrupt your configuration.

Parameter: Enable/Disable

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Enable

Options: Enable | Disable

Function: Enables or disables DCMMW (the DCM software subsystem) and therefore the DCM.

Instructions: To disable the DCM, select Disable. To reenable the DCM, select Enable. Use this parameter to reboot the DCM by disabling, then reenabling, DCMMW.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.3

Parameter: Boot Option

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Local

Options: Local | Download

Function: Specifies whether the DCM uses the image file in its own flash memory for booting or a boot image copied from the BayStack router's flash memory card to DCM shared memory.

Instructions: Select Local to specify the image file in DCM local flash memory as the DCM boot image. Select Download to specify an image file on the BayStack router's flash memory as the DCM boot image. You specify the downloaded image using the Image Name parameter.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.8

Parameter: Image Name

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: None, but you must specify an image name when the Boot Option parameter is set to Download

Options: An ASCII text string up to 255 characters

Function: Specifies an image file on the BayStack router's flash memory card. The image name must be a fully qualified file name, including both the volume and file name.

Instructions: Enter the volume and file name of the image that you want the DCM to boot, using the format *<volume_number:filename>*, for example, **1:dcm_image**.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.7

Parameter: Image Save Mode

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Save

Options: Save | No Save

Function: Specifies whether the DCM saves the active image to its local flash memory.

Instructions: To save the active DCM boot image file to the DCM local flash memory (overwriting the existing saved image), select Save. Select No Save if you do not want to save the DCM boot image file. The image remains in DRAM until the next time the DCM boots.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.9

Parameter: Configuration Mode

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Local

Options: Local | Shared Memory

Function: Specifies whether to use the configuration information in DCM shared memory (DRAM) or the configuration information saved on the DCM's flash memory.

Instructions: Select Local to use the default configuration information in the DCM local flash memory. Select Shared Memory to use the configuration information from the BayStack router's flash memory, stored in DCM DRAM.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.10

Parameter: Save Configuration Info

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Save

Options: Save | No Save

Function: Specifies whether to save the configuration information in DRAM to the DCM flash memory.

Instructions: Select Save to save the configuration information in DRAM to the DCM flash memory (overwriting the existing configuration file). Select No Save to avoid overwriting the DCM configuration file.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.11

Parameter: RMON Max Host

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: 500

Options: 100 to 8128

Function: Indicates the maximum number of host addresses to be collected in each entry of the RMON host control table. The maximum limit depends on the amount of flash memory available in the DCM. When the host control table reaches this maximum value, the DCM deletes entries based on an LRU (least recently used) algorithm.

Instructions: Recommended values, based on DCM memory configurations, are

-- 2 to 4 MB: 2048
-- 8 MB: 4096
-- 16 MB: 8128

To verify the number of configured hosts, check the MIB object wfDCMmwRMONHost using the Site Manager Statistics tool.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.12

Parameter: RMON Default Host

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Disable

Options: Enable | Disable

Function: Specifies whether to create the RMON host control table at every boot. Some RMON network management applications expect the DCM to set up a host configuration; others enable and disable their own host configurations during normal operations.

Note that the DCM allows only one instance of the host control table.

Instructions: Select Enable to create the RMON host control table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON host control table at boot time.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.13

Parameter: RMON Default Matrix

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: Disable

Options: Enable | Disable

Function: Specifies whether to create the RMON matrix control table at every boot. Some RMON network management applications expect the DCM to set up a matrix configuration; others enable and disable their own matrix configurations during normal operations.

Instructions: Select Enable to create the RMON matrix control table at the next (and every subsequent) reboot. Select Disable to disable default creation of the RMON matrix control table at boot time.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.14

Parameter: RMON Object Support

Path: Configuration Manager > Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM)

Default: RMON2

Options: RMON2 | RMON

Function: Determines the Ethernet DCM from which you want to collect RMON2 statistics. You use this parameter only when you have multiple Ethernet DCMs on a network running RMON2 and you need to choose which Ethernet DCM to collect RMON2 information from.

Instructions: Choose RMON2 to collect RMON2 statistics for the Ethernet DCM. Any other Ethernet DCMs default to RMON.

MIB Object ID: 1.3.6.1.4.1.18.3.3.2.16.2.1.15

Appendix C
RMON and RMON2 MIB Groups

This appendix defines the RMON and RMON2 MIB groups and provides information about RMON memory usage and interoperability issues. RMON functions are described without referring to the low-level details of the RMON MIB, which are described in RFC 1757 and RFC 2021.

This appendix contains the following information:

Topic	Page
RMON MIB Groups	C-1
RMON2 MIB Groups	C-6
Memory Requirements for RMON Groups	C-11

RMON MIB Groups

RMON provides information about layers 1 and 2 of the seven-layer OSI network model. You can monitor information on an Ethernet network through nine different MIB groups that comprise the RMON specification. RFC 1757 defines the function and organization of the RMON MIB groups.

Bay Networks implements the following MIB groups in its RMON agent for BayStack AN/ANH and ARN routers:

- Statistics
- History
- Host
- HostTopN
- Matrix

- Filter
- Capture

The router base module supports the following groups:

- Alarm
- Event

RMON MIB Group Controls and Functions

Several of the RMON groups in the MIB contain control and data tables. Control tables contain control parameters that specify which statistics you want to access and collect. You can view and change many entries in a control table. Data tables contain statistics the agent collects; usually you can only view entries in these tables.

The following sections describe the function of each group and the tables that each group defines. Refer to RFC 1757 for the following information:

- A list of all the parameters that appear in a control table
- The read/write status of a control parameter
- The default values for control parameters with read/write status
- A list of all the objects that appear in a data table

Statistics Group

The statistics group records data that the Ethernet DCM measures on network interfaces. The Ethernet DCM creates one entry for each Ethernet interface it monitors and places the entry in the EtherStatsTable. The EtherStatsTable also contains control parameters for this group.

History Group

The history group contains a control and data collection function. The control function manages the periodic statistical sampling of data from networks and specifies control parameters, such as the frequency of data sampling, in the historyControlTable.

The data collection function records periodic statistical samples from Ethernet networks, for example, interval start time and number of packets. This function places the statistical samples in the etherHistoryTable.

Host Group

The host group identifies hosts on the network by recording the source and destination MAC addresses in good packets, and places the information in the hostTable. This group also records the time it discovered a host on the network in the hostTimeTable. The hostControlTable specifies control parameters, such as which monitoring operations the Ethernet DCM performs, and contains some information about the monitoring process.

HostTopN Group

The HostTopN group ranks hosts according to a statistic type. For example, you can rank the hosts by the number of errors they generate. Control parameters for this group are stored in the hostTopNControlTable, and data this group generates is stored in the hostTopNTable. To use the HostTopN group, you must set up the host group.

Matrix Group

The matrix group stores statistics for an interchange between hosts at different addresses. This group's control parameters, such as number of hosts, are stored in the matrixControlTable. When the matrix group receives information from a good packet, it places data in both the matrixSDTable and the matrixDSTable.

Filter Group

The filter group specifies the types of packets the Ethernet DCM can capture. Filter control parameters, such as the minimum length of those packets, are stored in the filterTable. Associated with each filter is a *channel* (a specific path along which data flows). Control parameters in the channelTable define how and where the filtered packets flow.

Capture Group

The capture group enables the capture of packets that satisfy the filter group control parameters for a particular channel. Control parameters in the bufferControlTable specify how to transfer data from the channelTable to the captureBufferTable. For example, you can specify the maximum number of octets from each packet that the group can store in the captureBufferTable. To use the capture group, you must set up the filter group.

Alarm Group

The alarm group allows you to set an alarm threshold and a sampling interval to enable the RMON agent to generate alarms on any network segment it monitors. Alarm thresholds can be based on absolute or delta values, so that you can be notified of rapid spikes or drops in a monitored value.

Each alarm is linked to an event in the event group. An event defines an action that is triggered when the alarm threshold is exceeded.

The alarm group periodically takes statistical samples from variables in the Ethernet DCM and compares them to previously configured thresholds. The Alarm Table stores configuration entries that define a variable, a polling period, and threshold parameters. If the RMON agent determines that a sample crosses the threshold values, it generates an event. The RMON agent monitors any variables that resolve to an ASN.1 primitive type of integer (integer, counter, gauge, or TimeTick).

You can specify rising or falling thresholds, indicating network faults such as slow throughput or other network-related performance problems. You specify rising thresholds when you want to be notified that an alarm has risen above the threshold you specified. You specify falling thresholds when you want to be notified that the network is behaving normally again. For example, you might specify a falling threshold of 30 collisions per second to indicate a return to acceptable behavior.

When you configure an alarm condition, you must define the following values:

- The monitoring interval over which data is sampled
- The variable to be sampled
- Rising and falling thresholds to detect when network trouble starts and ends

- The event that takes place when a rising threshold is crossed
- The event that takes place when a falling threshold is crossed

Event Group

The event group allows for the generation of an SNMP trap, a log entry, or both, for any event you choose. An event can occur when the sample variable exceeds the alarm threshold or exceeds a channel match event generated on an Ethernet DCM. Traps can be delivered by the RMON agent to multiple management stations. For information about setting trap destinations, see *Configuring SNMP, BootP, DHCP, and RARP Services*.

You can set up events to either record the monitoring information or to notify the network management station. The event group includes an event table and a log table. The event table defines the notification that takes place when an event is triggered.

Each entry in the event table identifies an event that can be triggered and indicates an action. The event can trigger any of the following actions:

- The system sends an SNMP trap to the network management station.
- The management station is notified immediately. The management station determines how to react to the SNMP trap.
- The system logs the event in the log table in the agent system.
- The system sends an SNMP trap and logs the event in the log table.

The log table is a read-only data table for the network management station. It records each event that needs to be logged, including the event number, an index that distinguishes occurrences of the same event, the time at which the event occurred, and the event description. You are not required to configure the log table.

The management station can retrieve the information stored in the log table for further analysis. For example, the information collected can be used to select proper threshold values.

Event Trap Considerations

To allow RMON to generate trap events, you must set up the SNMP manager table. In the SNMP manager table, you add the SNMP community names that you configured for the network management application (for example, Optivity Analysis for Windows NT) and for the hosts on which you are running applications. If you do not make these changes, the router will be unable to send trap events to the network management station. See *Configuring SNMP, BootP, DHCP, and RARP Services* for instructions on how to set up an SNMP manager table.

When you set up the SNMP manager table, you can do one of the following: use the SNMP community names that the network management application uses and modify the trap-receiving tables on the router to use these names; or configure the router to use specific SNMP community names and modify the network management software to use these names.

When configuring SNMP community managers, you must assign each manager a specific IP address; you cannot specify a wildcard for the community manager address. Also, you must configure community managers to receive all traps, not just generic traps. You do this by changing the Trap Types parameter in the SNMP Manager window from Generic (the default) to All. For more information about changing communities and community manager parameters, see *Configuring SNMP, BootP, DHCP, and RARP Services*.

RMON2 MIB Groups

With RMON2, you can view traffic statistics by protocol and by application within the protocol to obtain an enterprise view of the network. RFC 2021 defines the function and organization of the RMON2 MIB groups.

Bay Networks implements the following seven groups in its RMON2 agent for BayStack AN/ANH and ARN routers:

- Protocol Directory
- Protocol Distribution
- Address Mapping
- Network Layer Host
- Application Layer Host

- Network Layer Matrix
- Application Layer Matrix

Protocol Directory Group

The Protocol Directory group lists the protocols that the Ethernet DCM can monitor. These protocols represent different network layer, transport layer, and higher-layer protocols.

Figure C-1 shows the statistics collected for the Protocol Directory group using the Threshold Manager tool in the Optivity Analysis application.

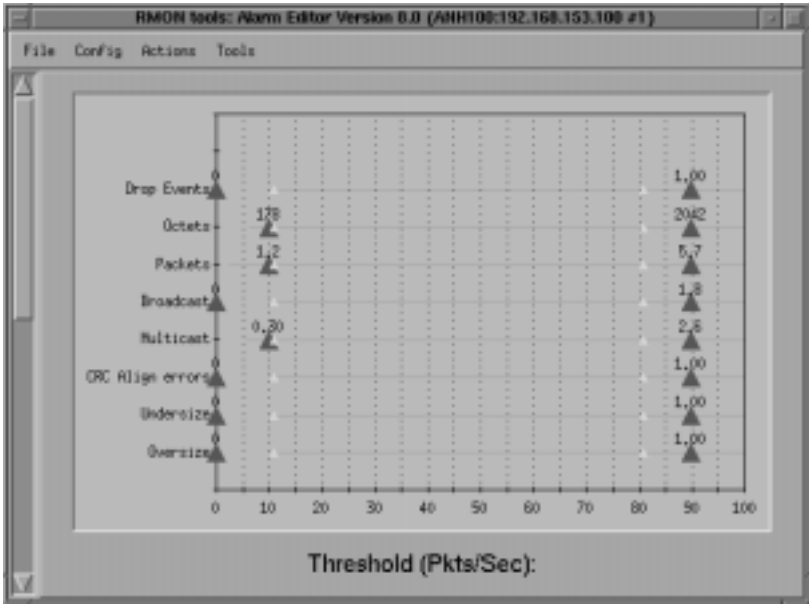

Figure C-1. Protocol Directory Statistics

Protocol Distribution Group

The Protocol Distribution group collects the relative numbers of octets and packets for the different protocols detected on a network segment. An RMON application can use this table to quickly determine bandwidth allocation used by different protocols. An entry is made in the table for every protocol in the Protocol Directory table that has been seen in at least one packet. Counters are updated in this table for every protocol type that is encountered when parsing a packet, but no counters are updated for packets with MAC-layer errors.

Figure C-2 shows the statistics collected for the Protocol Distribution group using the Optivity Analysis for Windows NT application.

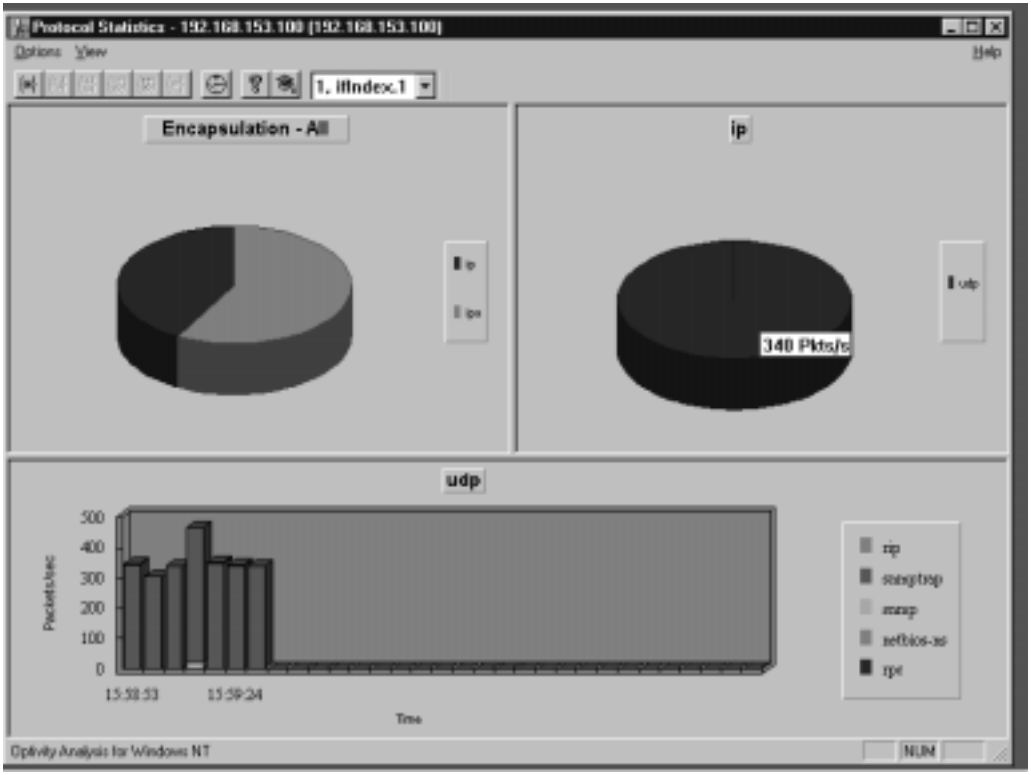

Figure C-2. Protocol Distribution Statistics

Address Mapping Group

The Address Mapping group maps network layer addresses to MAC layer addresses discovered by the Ethernet DCM. The network management application can correlate these network layer addresses to names via DNS or another naming utility. The Ethernet DCM creates entries in this table for all protocols that it understands. If it cannot perform address mapping for the protocol, or if this protocol is not a network layer protocol, then it does not interpret the addresses.

Network Layer Host Group

The Network Layer Host group records the amount of traffic sent to and from each network layer address discovered by the Ethernet DCM. These entries enable the collection of the network and application layer host tables indexed by network addresses. Entries in the network layer host table are created on behalf of each entry in this table. Additionally, if the Ethernet DCM implements the application layer host table, entries in that table are created on behalf of this table.

Application Layer Host Group

The Application Layer Host group records the amount of traffic, by protocol, sent from and to each network layer address discovered by the Ethernet DCM.

To implement this group, you must first implement the Network Layer Host group. The Ethernet DCM adds all addresses seen as the source or destination address in all packets with no MAC errors to the application layer host table, and increments octet and packet counts for all packets with no MAC errors.

Network Layer Matrix Group

The Network Layer Matrix group provides a table of traffic matrix entries that collect statistics for conversations between two network layer addresses. This table is indexed first by the source address and then by the destination address to make it convenient to collect all conversations from a particular address. The Ethernet DCM adds all pairs of addresses seen in all packets with no MAC errors to this table, and increments octet and packet counts for all packets with no MAC errors.

Application Layer Matrix Group

The Application Layer Matrix group provides a table of application layer traffic matrix entries, which collect statistics for conversations of a particular protocol between two network layer addresses. This table is indexed first by the source address and then by the destination address to make it convenient to collect all conversations from a particular address. The Ethernet DCM adds all pairs of addresses seen in all packets with no MAC errors to this table, and increments octet and packet counts for all packets with no MAC errors. To implement this group, you must first implement the Network Layer Matrix group.

Figure C-3 shows the statistics collected for the Application Layer Matrix group using the Optivity Analysis for Windows NT application.

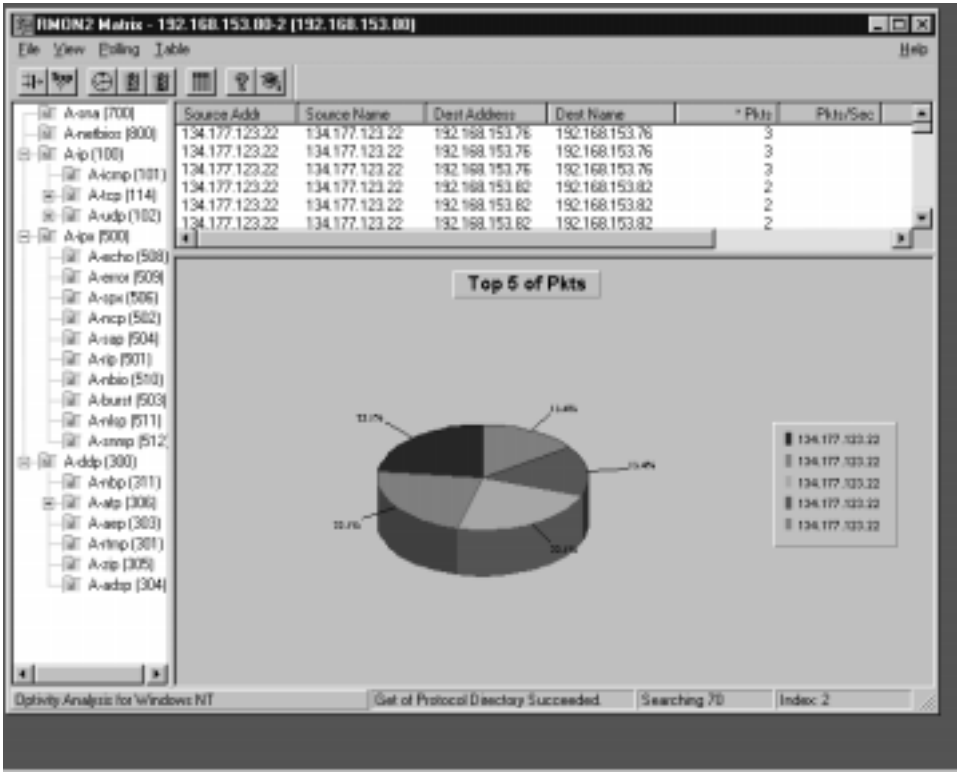

Figure C-3. Application Layer Matrix Statistics

Memory Requirements for RMON Groups

To optimize the use of your network management applications (such as Optivity Analysis for Windows NT), you need to understand each RMON group's memory requirements.

The total amount of available RMON and RMON2 memory depends on the DRAM available on the Ethernet DCM (Table C-1).

Table C-1. DRAM and RMON Memory Size

Installed DRAM (MB)	Available RMON Memory in Bytes
4	2,077,330
8	5,222,034
16	12,561,042

Note: If the RMON memory pool is full or if the RMON agent reaches an implementation limit, the agent responds to an SNMP **set** command on an RMON control table entry with an SNMP GEN-ERROR.

The following sections describe how much memory you need to:

- Configure an RMON group (for example, the matrix group or the filter and capture groups).
- Store the data for an RMON group (for example, the packets on Ethernet DCM captures).

In the following sections, the term *configuration* means the set of control tables for a group. For example, a matrix configuration includes only the matrixControlTable. Note that you can create more than one configuration for some RMON groups. For example, you can create more than one history configuration, allowing you to specify different intervals for sampling statistics.

Statistics Group

When you enable the Ethernet DCM, the RMON agent automatically creates a statistics configuration that records data for each network interface. Through your RMON network management application, you can create as many statistics configurations as memory permits, up to the RMON limit of 65,535 configurations.

If you create multiple configurations, it is possible to collect the same set of statistics for the same interface in multiple data tables. The absolute values of those statistics may vary from table to table, because the baseline of each statistics counter occurs when you create a configuration. You may prefer, however, to use only one statistics configuration, to conserve memory for other RMON groups.

You need 200 bytes of memory for each statistics configuration.

History Group

When you enable the Ethernet DCM, the RMON agent automatically creates a history configuration that collects history data at two intervals. The first configuration provides short-term history by sampling statistics every 30 seconds and holding up to 50 samples (called *buckets*). The second configuration provides long-term history by sampling statistics every 30 minutes and holding up to 50 buckets.

Warning: Through your RMON network management application, you can create as many history configurations as memory permits, up to the RMON limit of 65,535 configurations. You can also set the number of buckets for a particular history configuration to as many as available memory allows. If you request more buckets than memory allows, the agent allocates enough buckets to fill available memory.

You need 504 bytes of memory for each history configuration (252 bytes each for the short-term and long-term history configurations).

The history data requires 52 bytes of memory per bucket. You calculate the total memory (in bytes) you need to store the data as follows:

number of buckets * 52 * 2 history configurations

This calculation shows that you need approximately 5.1 KB for the default setting of 50 buckets.

Host Group

When you enable the Ethernet DCM, the default setting for the RMON Default Host parameter is Disable, meaning that no host configuration is created. To create a host configuration, set the RMON Default Host parameter to Enable (see "Modifying Default RMON MIB Group Parameters" on page 4-12).

Some RMON network management applications expect the Ethernet DCM to set up a host configuration, but others set up their own configurations.

Note: The RMON agent allows you to create only one host configuration. Make sure to set the RMON Default Host parameter according to the expectations of the RMON network management application.

The host configuration requires 148 bytes. The host data requires 105 bytes of memory per host address that the Ethernet DCM detects on a segment.

You specify the maximum number of host addresses that appear in the host configuration by setting the RMON Max Host parameter. If there is not enough memory for the number of hosts you request, the RMON agent sets the RMON Max Host parameter to the highest possible value. The number of addresses can range from 100 to 8,128 hosts, depending on the Ethernet DCM memory configuration. Table C-2 shows recommended values for this parameter.

Table C-2. Maximum Number of Hosts

Installed DRAM (MB)	Maximum Hosts
2-4	2,048
5-8	4,096
9-16	8,128

You calculate the total memory (in bytes) you need for the host data as follows:

105 * value of the RMON Max Host parameter

HostTopN Group

To save memory and increase performance, there is no default configuration for the HostTopN group. You must create HostTopN configurations through your RMON network management application. You can create as many HostTopN configurations as memory permits, up to the RMON limit of 65,535 configurations.

Note: Before you create a HostTopN configuration, you must create a host configuration.

Each HostTopN configuration requires 164 bytes. The HostTopN data requires 10 bytes of memory per host address that the Ethernet DCM detects on a segment.

You calculate the total memory (in bytes) you need for the HostTopN data as follows:

10 * value of the RMON Max Host parameter

For information about setting the RMON Max Host parameter, see “Modifying Default RMON MIB Group Parameters” on page 4-12.

Matrix Group

When you enable the Ethernet DCM, the default setting for the RMON Default Matrix parameter is Disable. To create a matrix configuration, set the RMON Default Matrix parameter to Enable (see “Modifying Default RMON MIB Group Parameters” on page 4-12).

Some RMON network management applications expect the DCM to set up a matrix configuration, but others set up their own configurations.

Note: The RMON agent allows you to create only one matrix configuration. Make sure to set the RMON Default Matrix parameter according to the expectations of the RMON network management application.

The matrix configuration requires 212 bytes. The matrix data requires approximately 178 bytes of memory per source/destination pair that the Ethernet DCM detects on a segment.

Filter and Capture Groups

Caution: The memory you need for a filter/capture configuration and for storing captured packets can easily exhaust all the available memory on an Ethernet DCM, particularly if the filters are not selective.

You must create filter and capture configurations through your RMON network management application. You can create as many filters and capture buffers as memory permits, up to the RMON limit of 65,535 configurations.

Memory requirements vary greatly according to the size and number of the filters and the size of the capture buffer. In most cases, you need 3 to 5 KB of memory for the filter and capture configuration.

The size of the capture buffer determines the amount of memory you need for the data. You can request the largest buffer size available by specifying a buffer size of -1 through your RMON network management application. When you specify -1 for the capture buffer size, the agent attempts to allocate a default buffer, depending on the DRAM in the Ethernet DCM (Table C-3).

Table C-3. Default Size for Capture Buffer

Installed DRAM (MB)	Default Buffer Size (KB)
4	64
8	256
16	512

You can also request a larger buffer size up to 15 MB. In any case, if there is not enough memory currently available to satisfy the request, the agent will provide a buffer that uses all available memory.

You can determine the maximum number of packets that an agent can capture in a buffer as follows:

buffer size/(packet slice size + 20 bytes)

Example

You specify a buffer size of 32 KB and a packet slice size of 1 KB. After checking the available memory, the RMON agent allocates the buffer size you requested. The buffer can hold a maximum of 32,768 / (1024 + 20), or 31 packets.

Note: The RMON agent allocates the full amount of memory you specify for the packet slice size to each packet, even if the packet size is smaller than this amount. For this reason, Bay Networks recommends that you set the packet slice size to the smallest size possible. The maximum packet size is 2 KB.

Alarm and Event Groups

When you enable the Ethernet DCM, the router does not create default alarm or event entries. Bay Networks recommends that you create alarm and event entries using a network management application, such as Optivity Analysis for Windows NT.

You can create as many alarm and event entries as memory permits, up to the RMON limit of 65,535 entries. The memory limitation for alarm and event groups is based on the memory resources allocated on the router base module rather than on the Ethernet DCM. The RMON alarm and event groups are maintained by the router base module. All other RMON groups are supported on the Ethernet DCM.

Each alarm entry requires 232 bytes. Each event entry requires 542 bytes.

The log table can accommodate up to 65,535 entries. Each entry in the log table requires 267 bytes. You cannot delete log entry rows. Therefore, as events are triggered and the event type specifies logging, the log table increases in size. Although there is no way to delete a specific log entry, all log entries in the log table corresponding to a single event entry are deleted when the event entry is deleted.

Appendix D
Upgrading the DCM Software Image

This appendix describes how to upgrade the DCM software image on BayStack routers using Site Manager or the Technician Interface. This appendix includes the following information:

Topic	Page
Verifying Minimum DCM Requirements	D-1
Upgrading the DCM Software Image	D-2

Verifying Minimum DCM Requirements

To verify the minimum DCM hardware and software requirements:

1. **Establish a Technician Interface session on the router.**
2. **Verify the correct DCM hardware revision by entering the following command:**

   [1:TN]$ get wfDCMEntry.wfDCMhwRev.*

   The Technician Interface displays information similar to the following:

   ```
   wfDCMEntry.wfDCMhwRev.1 = "E"
   wfDCMEntry.wfDCMhwRev.2 = "E"
   ```

   If the Hardware Revision line indicates “C” or earlier, you must upgrade to DCM Hardware Revision E.

3. **Display the current version of DCM agent software.**

   Your version of router software determines which command you enter:

   - For a router running Router Software Version 11.0 or later, enter the following command to display the DCM agent software version:

     [1:1]$ get wfDCMEntry.wfDCMagentImageVersion.*

     The Technician Interface displays information similar to the following:

     ```
     wfDCMmw.wfDCMagentImageVersion.1 = ”V1.4.2“
     ```

     (There are two entries if there are two DCMs installed on an ARN router.)

   - For an AN or ANH router running Router Software Version 9.0 or 10.0*x*, enter the following command:

     [1:TN]$ get wfDCMmw.wfDCMAgentImageVersion.0

     The Technician Interface displays information similar to the following:

     ```
     wfDCMmw.wfDCMAgentImageVersion.0 = ”V1.4.2“
     ```

   If the Agent Image Version line does not indicate “V1.4.1” or “V1.4.2,” go to the next section to upgrade the DCM agent software.

Upgrading the DCM Software Image

Upgrading the DCM software image in BayStack routers involves the following tasks:

- Transferring the DCM software image from CD to your PC or UNIX workstation
- Transferring the DCM software image from your PC or UNIX workstation to the router’s flash memory card
- Transferring the DCM software image from the router’s flash memory to the DCM’s flash memory

Using Site Manager

To upgrade the DCM software image in a BayStack router using Site Manager:

1. **Transfer the DCM software image (for example, *in_2.00.1.obj*) to a PC or UNIX workstation from:**

   - The latest BayRS CD release media
   - The World Wide Web URL:

     http://support.baynetworks.com/software/Router/

   Contact the Bay Networks Technical Solutions Center if you do not have access to these sources.

2. **Transfer the DCM software image from your PC or workstation to the router's flash memory.**

   Use the Site Manager Router Files Manager utility.

3. **Transfer the DCM software image from the router's flash memory to the DCM flash memory, as follows:**

   In the Configuration Manager window (Figure D-1), choose Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM).

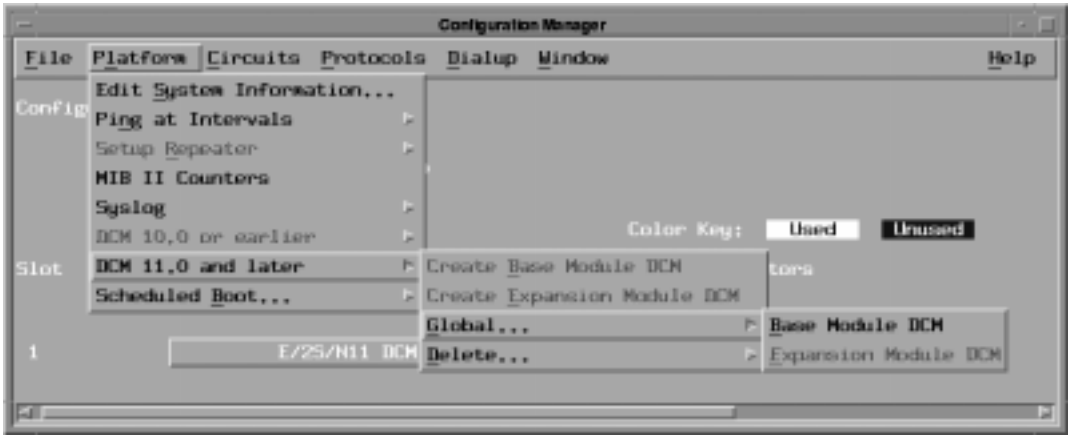

Figure D-1. Choosing DCMMW Global Configuration Parameters

The Edit Base Module DCM Parameters window opens (Figure D-2).

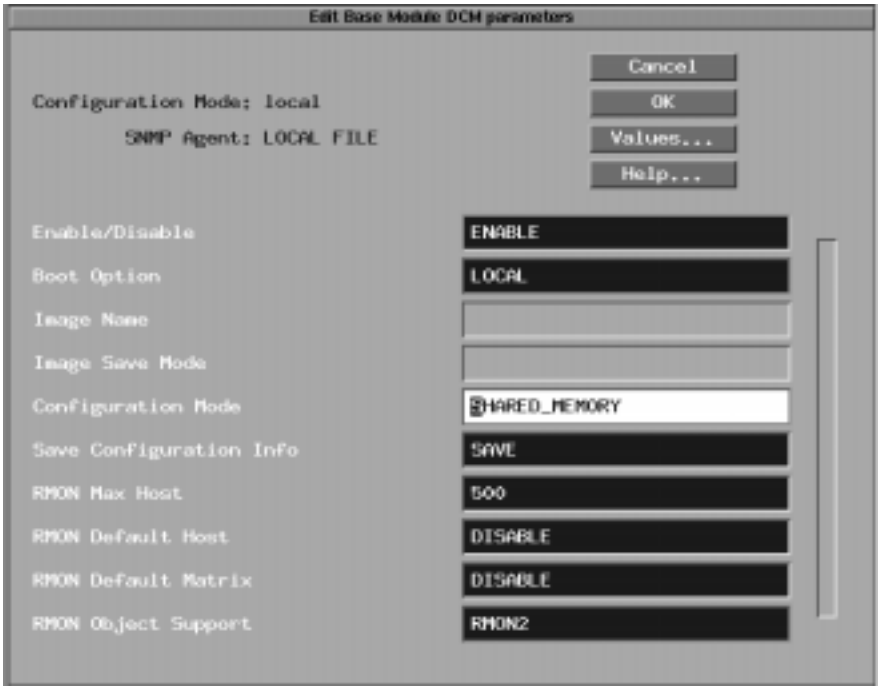

Figure D-2. Edit Base Module DCM Parameters Window

4. **Set the Enable/Disable parameter to Disable.**
5. **Change the Boot Option from Local to Download.**

   This setting specifies that you want the Ethernet DCM to boot the downloaded DCM image from the router's shared memory instead of from the Ethernet DCM's flash memory.
6. **In the Image Name field, specify the target volume and the file name of the new DCM software image (*in_2.00.1.obj*) on the router, for example:**

   1: in_2.00.1.obj
7. **Set the Image Save Mode parameter to Save and click on OK.**

   You return to the Configuration Manager window.

If you set the Image Save Mode parameter to No Save, the Ethernet DCM boots with the new software image but does not save the image to the Ethernet DCM's flash memory.

8. **In the Configuration Manager window (Figure D-1), choose Platform > DCM 11.0 and later > Global > Base Module DCM (or Expansion Module DCM).**

   The Edit Base Module DCM Parameters window opens (Figure D-2).

9. **Set the Enable/Disable parameter to Enable and click on OK.**

   This action boots the Ethernet DCM with the new DCM software image that you specified using the Image Name parameter and saves the new DCM software image to flash memory, if specified.

10. **Set the Boot Option parameter to Local.**

    Choose the Local option after you save the DCM software image to the Ethernet DCM's flash to boot the Ethernet DCM from its own flash memory.

11. **Click on OK.**

Using the Technician Interface

To upgrade the DCM software image in a BayStack router using the Technician Interface:

1. **Transfer the DCM software image (for example, *in_2.00.1.obj*) to a PC or UNIX workstation from:**

   - The latest BayRS CD release media
   - The World Wide Web URL:

     http://support.baynetworks.com/software/Router

   Contact the Bay Networks Technical Solutions Center if you do not have access to these sources.

2. **Use FTP or TFTP to transfer the DCM image file and the Technician Interface script dcmload.bat from the workstation to the flash memory card on the router.**

3. **Enter the following Technician Interface command to download the new software image from the router flash memory card to the DCM flash memory:**

   `[1:1]$` **dcmload**

   The Technician Interface displays information about the **dcmload** script and displays the following prompt:

   ```
   Do you want to download an image to the Base Module DCM
   or the Expansion Module DCM (b/e) [b]
   ```

4. **If the DCM is installed on the base module, press Return. If the DCM is installed on an ARN expansion module, enter e.**

   The Technician Interface displays the following prompt:

   ```
   Specify DCM image name (volume:filename):
   ```

5. **Enter the image name in the form** *<volume:filename>.*

   Volume is 1 and *filename* is the name you gave the DCM image during the file transfer.

   For example, enter:

   1: in_2.00.1.obj or 1:dcm201image.

   The Technician Interface displays the following prompt:

   ```
   Do you want DCM to save this image on its FLASH? (y/n) [y]
   ```

6. **Answer yes by pressing [Return].**

   If you answer no, the DCM uses the downloaded image only once, reverting to the previous image at the next boot. The Technician Interface displays the following prompt:

   ```
   Do you want to start the download process? (y/n)[y]
   ```

7. **Answer yes to begin downloading the new image, overwriting the existing DCM software image.**

   The downloading process takes less than 1 minute.

8. **Verify that the DCM software image is now Version 2.00.1.**

   See step 3 in the earlier section, "Verifying Minimum DCM Requirements," on page D-1.

Sample Display: dcmload.bat

```
    Use this script to download a DCM image from the router's
    Flash to a DCM board.

    When prompted for the image file name, use the form
    <volume:filename>.

    When prompted whether to save the image on the DCM Flash,
    answer yes (y) to overwrite the existing image on the DCM
    Flash with the new image. Answer no (n) to use the downloaded
    image once, but lose it at the next boot.

Specify DCM image name (volume:filename): 1:in_2.00.1.obj

Do you want DCM to save this image on its FLASH? (y/n) [y]: y

Image Name is 1:dcmboot.exe
Image will be saved by DCM in its FLASH

Do you want to start the download process? (y/n) [y]: y
Downloading of DCM image has started. It will take few seconds to
complete.
```

Index

A

acronyms, xv

address mapping group, RMON2, C-9

alarm group, RMON
- described, C-4
- memory requirements, C-16

application layer matrix group, RMON2, C-10

B

Boot Option parameter, B-2

C

capture group, RMON
- described, C-4
- memory requirements, C-15

configuration files
- preparing for AN/ANH and ARN, 2-4
- preparing for ARN 100, 3-3
- setting the save mode, 4-6

Configuration Mode parameter, B-4

conventions, text, xiv

customizing DCM parameters, 4-1

D

data collection module middleware (DCMMW), 1-9

DCM (data collection module)
- configuring
  - AN/ANH, 2-5
  - ARN, 2-8
- customizing parameters, 4-12
- DCM software image, D-3
- deleting software subsystem, 4-19
- disabling, 4-2
- enabling
  - AN/ANH, 2-5, 2-7
- rebooting, 4-18
- requirements, hardware and software, 2-2
- saving configuration information, 4-8
- setting for RMON or RMON2, 4-3

DCM agent software
- described, 1-11
- displaying current version, D-1
- upgrading, D-2

DCM boot image
- setting the save mode, 4-6
- upgrading
  - using Site Manager, D-3
  - using the Technician Interface, D-5

dcmload command, D-7

DCMMW (DCM middleware)
- customizing parameters, 4-1
- deleting, 4-19
- disabling, 4-2
- reenabling, 4-18

E

educational services, xvi

Enable/Disable parameter, B-2

Ethernet DCM parameters, B-1

event group, RMON
- described, C-5
- memory requirements, C-16

F

filter group, RMON
- described, C-3
- memory requirements, C-15

H

hardware requirements
  AN/ANH, 2-2
  ARN, 2-3
history group, RMON
  described, C-2
  memory requirements, C-12
host group, RMON
  described, C-3
  enabling host configuration, 4-14
  memory requirements, C-13
HostTopN group, RMON
  described, C-3
  memory requirements, C-14

I

Image Name parameter, B-3
Image Save Mode parameter, B-3
interoperability issues for RMON, C-11

M

matrix group, RMON
  described, C-3
  enabling matrix configuration, 4-16
  memory requirements, C-14
memory use for RMON, C-11
mini-RMON, 3-1

N

network layer host group, RMON2, C-9
network layer matrix group, RMON2, C-9

O

Optivity Analysis for UNIX, 1-12
Optivity Analysis for Windows NT, 1-16
Optivity LAN, 1-15

P

product support, xvi
protocol directory group, RMON2, C-7
protocol distribution group, RMON2, C-8
publications, Bay Networks, xvi

R

RFC 1757, 1-1
RFC 2021, 1-11
RMON
  control parameters, C-2
  control tables, C-2
  data tables, C-2
  interoperability issues, C-11
  memory use, C-11
RMON Default Host parameter, B-5
RMON Default Matrix parameter, B-6
RMON Max Host parameter, B-5
RMON MIB
  described, 1-1
  modifying RMON default parameters, 4-12
RMON MIB groups, 1-2, C-4
RMON network management software
  described, 1-12
  implementation of RMON MIB groups, C-11
RMON Object Support parameter, B-6
RMON/RMON2
  Bay Networks implementation, 1-8
  components, 1-9
  customizing parameters, 4-3
  specifying data collection type, 4-3
  starting
    AN/ANH, 2-4
    ARN, 2-8
    preparing a configuration file, 2-4
RMON2, 1-3
RMON2 MIB groups
  described, 1-5
RMON2 MIB groups, described, C-6

router hardware and software requirements
AN/ANH, 2-2
ARN, 2-3

S

Save Configuration Info parameter, B-4
show commands
ethernet, A-2
Simple Network Management Protocol (SNMP), 1-1
software requirements
AN/ANH, 2-2
ARN, 2-3
statistics group, RMON
described, C-2
memory requirements, C-12
support, Bay Networks, xvi

T

technical publications, xvi
technical support, xvi
text conventions, xiv

U

upgrading DCM boot image
determining need for, D-1
using Site Manager, D-3
using Technician Interface, D-5